Exhibit 1 to Mao Decl.
Fourth Amended Complaint

Redacted Version

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted *pro hac vice*)
Rossana Baeza (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsfllp.com
rbaeza@bsfllp.com

Amanda K. Bonn, CA Bar No. 270891
SUSMAN GODFREY L.L.P
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

John A. Yanchunis (admitted *pro hac vice*)
Michael F. Ram, CA Bar No. 104805
Ryan J. McGee (admitted *pro hac vice*)
Ra Amen (admitted *pro hac vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

William S. Carmody (admitted *pro hac vice*)
Shawn Rabin (admitted *pro hac vice*)
Steven M. Shepard (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019-6023
Tel.: (212) 336-8330
Fax: (212) 336-8340
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, SAL CATALDO, JULIAN SANTIAGO, and SUSAN LYNN HARVEY, individually and on behalf of all other similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 3:20-cv-04688-RS

FOURTH AMENDED COMPLAINT

CLASS ACTION FOR
(1) VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE §§ 502 *ET SEQ.*;
(2) INVASION OF PRIVACY;
(3) INTRUSION UPON SECLUSION

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

FOURTH AMENDED CLASS ACTION COMPLAINT

Plaintiffs Anibal Rodriguez, Sal Cataldo, Julian Santiago, and Susan Lynn Harvey, individually and on behalf of all others similarly situated, file this Fourth Amended Class Action Complaint against defendant Google LLC ("Google" or "Defendant"), and in support state the following.

INTRODUCTION

"*I want people to know that everything they're doing online is being watched, is being tracked, is being measured. Every single action you take is carefully monitored and recorded.*"

-Jeff Seibert; Former Head of Consumer Product of Twitter[1]

1. This case is about Google's surreptitious interception, collection, saving, and use of consumers' highly personal browsing histories on their mobile devices, whenever consumers use certain software applications ("apps") that have incorporated Google code. Google did this without notice or consent, where Plaintiffs had turned off a Google feature called "Web & App Activity" ("WAA") or a sub-setting within WAA known as "supplemental Web & App Activity" ("sWAA"). Google had promised that by turning off this feature, users would stop Google from saving their web and app activity data, including their app-browsing histories. Google's promise was false.

2. Google has said, over and over again, that it values privacy and gives users control. The truth is just the opposite. Google continues to track users and collect their data even after users follow Google's instructions on how to stop that tracking and collection. What Google calls its privacy "controls" are ruses. These Google features are intended to lull users—along with regulators, legislators, and app developers—into a false sense of control and privacy. In reality, no matter what users do, Google never stops intercepting, collecting, tracking, and using users' app-browsing data. [redacted]

[1] *The Social Dilemma*, NETFLIX (Jan. 2020), https://www.netflix.com/title/81254224?s=i&trkid=13747225.

[redacted]

3. Google surreptitiously collected users' personal data from their mobile devices using software scripts embedded in Google's Firebase SDK development platform. Third-party software developers then used Firebase SDK to build their apps (as Google coerced them to do). Users downloaded and used those apps to communicate with third parties (e.g., The New York Times app allows users to communicate with The New York Times) through their mobile devices. Unknown to users, the Firebase SDK scripts still copied users' communications and transmitted them to Google's servers through the users' devices, to be saved and used by Google for Google's purposes. Google did all this even if users switched off Google's "Web & App Activity" feature, without providing any notice or obtaining any consent.

[redacted]

6. Google repeatedly told its users that if they "turn off" the "Web & App Activity" feature, then that would stop Google from "sav[ing]" the users' app data. [redacted]

[redacted] Similarly, Google presented such settings to their business partners as device level controls, including by requiring the controls and accompanying representations written by Google as part of the Android operating systems ("Android OS") licensed to Android device manufacturers, such as Samsung.

7. Google's Privacy Policy also promised users control. That Privacy Policy states, on the first page:

> When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and ***put you in control***.
> . . . .
> Our ***services*** include: … ***products that are integrated into third-party apps*** and sites, like ads and embedded Google Maps.
> . . . .
> ***[A]cross our services, you can adjust your privacy settings to control what we collect and how your information is used***.

That language is quite plain. Any reasonable person would understand it to mean just what it says: the user "can adjust . . . privacy settings to control what [Google] collects and how [user] information is used" by Google "across [Google's] services," which services "include . . . products," like Google's Firebase SDK platform [redacted] "that are integrated into third-party apps."

8. In fact, Google still collects data from users who turn off the "Web & App Activity" feature. Google collects this data through various backdoors made available through and in connection with Google's Firebase Software Development Kit, including not only Google Analytics for Firebase but also without limitation AdMob and Cloud Messaging for Firebase. [redacted] All of these products surreptitiously copy and provide Google with app activity data while WAA is turned off, including personal browsing data.

9. Google accomplishes this surreptitious interception and collection using mobile devices to copy data from user communications with non-Google branded apps via and in

connection with Google's Firebase SDK, including through background data collection processes such as Android's Google Mobile Service. Through discovery in this case, Plaintiffs are only now beginning to understand the full scope of Google's unlawful data collection practices while WAA is turned off, [redacted]

10. Google's employees recognize, internally and without disclosing this publicly, that WAA is "***not clear to users***" (GOOG-RDGZ-00021182), "***nebulous***" (GOOG-RDGZ-00014578), "***not well understood***" (GOOG-RDGZ-00020706), [redacted] and "***confuses users***" (GOOG-RDGZ-00015004), where people "***don't know what WAA means***" (GOOG-RDGZ-00021184) and Google's promise of control is "***just not true***" (GOOG-RDGZ-00020680). Google employees accordingly describe WAA [redacted]

11. This is especially true in terms of turning WAA off, with Google employees admitting "***we don't accurately describe what happens when WAA is off***" (GOOG-RDGZ-00024690) and acknowledging that WAA "does not actually control what is stored by Google" which "is ***really bad***" because turning WAA off leaves users with a "***false sense of security*** that their data is not being stored at Google, when in fact it is" (GOOG-RDGZ-00024698). As aptly summarized by different Google employees:

[redacted]

12. Google has continued to engage in this illegal data collection even after Plaintiffs filed this lawsuit, with Google using the data it collects to create profiles and generate billions of dollars in revenues and other benefits. Google could have disclosed its collection and use of this data, while Web & App Activity is turned off, but Google chose not to. Instead, Google intentionally created an illusion of user control.

13. Because of its pervasive and unlawful interceptions of this data, Google knows users' friends, hobbies, political leanings, culinary preferences, cinematic tastes, shopping activity, preferred vacation destinations, romantic involvements, and even the most intimate and potentially embarrassing aspects of the user's app usage (such as medical issues).

14. Google's practices affect millions of Americans who care about protecting their privacy. According to Google, more than 200 million people visit Google's "Privacy Checkup" website each year. Each day, nearly 20 million people check their Google privacy settings. People do this because they care about their privacy and believe that they can "control" what Google collects (because Google has told them so). The truth is that Google's so-called "controls" are meaningless. Nothing stops Google from collecting this data, data Google then monetizes for its own benefit.

15. Google's practices unlawfully infringe upon consumers' privacy rights, give Google and its employees power to learn intimate details about individuals' lives, and make Google a potential target for "one-stop shopping" by any government, private, or criminal actor who wants to invade individuals' privacy.

16. Google must be held accountable for the harm it has caused. Google must be prevented from continuing to engage in its covert data collection from the mobile devices now in use by nearly every American citizen. Both federal and state privacy laws recognize and protect

individuals' reasonable expectations of privacy in confidential communications under these circumstances, and these laws prohibit Google's unauthorized interception and subsequent use of these communications.

17. Plaintiffs are individuals who had WAA turned off but whose devices nonetheless transmitted data to Google as a result of Google [redacted] embedded within non-Google apps (including but not limited to Firebase SDK scripts) and/or whose information related to interactions with [redacted] was saved by Google. Plaintiffs bring California state law claims on behalf of other similarly situated Google subscribers in the United States (the "Classes," defined herein in paragraph 257). The Class Period begins on the date Google first received data, as a result of [redacted], from the device of a user who had turned off WAA and/or sWAA. The Class Period continues through the present.

THE PARTIES

18. Plaintiff Anibal Rodriguez is an adult domiciled in Homestead, Florida. He had active Google accounts during the Class Period.

19. Plaintiff Sal Cataldo is an adult domiciled in Sayville, New York. He had active Google accounts during the Class Period.

20. Plaintiff Julian Santiago is an adult domiciled in Miami, Florida. He had an active Google account during the Class Period.

21. Plaintiff Susan Lynn Harvey is an adult domiciled in Madera, California. She had active Google accounts during the Class Period.

22. Defendant Google LLC is a Delaware limited liability company with a principal place of business at what is officially known as The Googleplex, 1600 Amphitheatre Parkway, Mountain View, California 94043. Google LLC regularly conducts business throughout California and in this judicial district. Google LLC is one of the largest technology companies in the world and conducts product development, search, and advertising operations in this district.

JURISDICTION AND VENUE

23. This Court has personal jurisdiction over Defendant because Google's principal place of business is in California. Additionally, Defendant is subject to specific personal

jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiffs' and Class members' claims occurred in this State, including Google servers in California receiving the intercepted communications and data at issue, and because of how employees of Google in California reuse the communications and data collected.

24. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, and at least one Class member is a citizen of a state other than California or Delaware.

25. Venue is proper in this District because a substantial portion of the events and actions giving rise to the claims in this matter took place in this judicial District. Furthermore, Google is headquartered in this District and subject to personal jurisdiction in this District.

26. Intradistrict Assignment. A substantial part of the events and conduct which give rise to the claims herein occurred in Santa Clara County.

FACTUAL ALLEGATIONS REGARDING GOOGLE

I. Google Has a Long History of Invading Consumers' Privacy and Misrepresenting the Scope of Google's Data Collections

27. For at least the last decade, Google has been persistently and pervasively violating consumers' privacy rights. The pattern is always the same. Google gets caught. Google gets punished. Google lulls consumers into a false sense of security again.

28. In 2010, the FTC charged that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz." To resolve these claims, Google, in 2011, agreed to the FTC's entry of a binding Order (the "Consent Order"), which barred Google "from future privacy misrepresentations" and required Google "to implement a comprehensive privacy program."[2] The Consent Order also required Google to take steps relating to "covered information," defined as "information [Google] collects from or about an

[2] *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network*, FED. TRADE COMM'N (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz (last visited Nov. 11, 2020).

individual."[3] The FTC ordered as follows:

> **I.**
>
> **IT IS ORDERED** that [Google], in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:
>
> A. the extent to which [Google] maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information…[4]
>
> **II.**
>
> **IT IS FURTHER ORDERED** that [Google], prior to any new or additional sharing by respondent of the Google user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, shall:
>
> A. Separate and apart from any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, clearly and prominently disclose: (1) that the Google user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing; and
>
> B. Obtain express affirmative consent from the Google user to such sharing.

29. Google quickly recidivated. Just one year after entry of the Consent Order, the FTC found that Google had already violated it. In an August 2012 press release, the FTC explained that Google had been promising users of Apple's Safari web browser that Google would not track their web browsing, and that Google had then broken those promises by "circumventing the Safari

---

[3] The term "covered information" thus includes, but is not limited to, "(c) online contact information, such as a user identifier . . . (d) persistent identifier, such as IP address . . . (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above."

[4] Agreement Containing Consent Order, *In re Google Inc.*, No. 1023136 (F.T.C.), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf (emphasis added).

browser's default cookie-blocking setting":

> Google Inc. has agreed to pay a record $22.5 million civil penalty to settle Federal Trade Commission charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC.
>
> The settlement is part of the FTC's ongoing efforts make sure companies live up to the privacy promises they make to consumers, and is the largest penalty the agency has ever obtained for a violation of a Commission order. In addition to the civil penalty, the order also requires Google to disable all the tracking cookies it had said it would not place on consumers' computers.
>
> "The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order," said Jon Leibowitz, Chairman of the FTC. "No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place."[5]

30. Since 2012, a number of federal, state, and international regulators have similarly accused Google of violating its data-collection and privacy promises, with Google failing to disclose and obtain consent for its conduct.

31. In January 2019, France's data privacy authority, known as the CNIL, fined Google $57 million for privacy violations. The violations related to: Google's lack of transparency regarding its data collection practices; Google's lack of valid consent from consumers; and the failure of Google's privacy settings to enable consumers to exercise real control over what Google collected.[6] In June 2020, France's highest court upheld this $57 million fine against Google, noting Google's failure to provide clear notice and obtain users' valid consent to process their personal data for ad personalization purposes on the Android mobile operating system. Google responded by stating that it had "'invested in industry-leading tools' to help its users 'understand and control

---

[5] *Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (last visited Nov. 11, 2020).

[6] Tony Romm, *France Fines Google $57 Million Under New EU Data-Privacy Law*, LOS ANGELES TIMES (Jan. 21, 2019), https://www.latimes.com/business/technology/la-fi-tn-google-france-data-privacy-20190121-story.html (last visited Nov. 11, 2020) (repost).

how their data is used.'"[7]

32. In September 2019, Google and its YouTube subsidiary agreed to pay $170 million to settle allegations by the FTC and the New York Attorney General that YouTube illegally collected personal information from children without their parents' consent.[8]

33. Proceedings by the Arizona Attorney General and the Australian Competition and Consumer Commission have also alleged that Google failed to obtain consent regarding its collection of location data and regarding its practices of combining certain user data.

34. In the Arizona Attorney General action, Google has produced documents establishing "overwhelming" evidence that "Google has known that the user experience they designed misleads and deceives users." Google's employees made numerous admissions in internal communications, recognizing that Google's privacy disclosures are a "mess" with regards to obtaining "consent" for its data-collection practices and other issues relevant in this lawsuit. Some of these documents were made publicly available on August 21, 2020 (ironically, with heavy privacy redactions by Google).

35. Some of the documents produced by Google in the Arizona Attorney General action refer to Google's "Web & App Activity" feature by name. These documents indicate that Google has long known that Google's disclosures about this feature were (at a minimum) highly confusing and insufficient to allow consumers to give informed consent. *See infra*, ¶¶ 104-05.

36. In an Australia proceeding, the Australian Competition & Consumer Commission ("ACCC") alleges that "Google misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers' internet activity, for use by Google, including for targeted advertising." The ACCC alleges that Google impermissibly combined the data it collected directly from consumers with data that it received

---

[7] The Associated Press, *Google Loses Appeal Against $56 Million Fine in France*, ABC NEWS (June 19, 2020), https://abcnews.go.com/Business/wireStory/google-loses-appeal-56-million-fine-france-71347227 (last visited Nov. 11, 2020).

[8] *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, FED. TRADE COMM'N (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (last visited Nov. 11, 2020).

from "third-party sites and apps not owned by Google." The ACCC contends that Google "misled Australian consumers about what it planned to do with large amounts of their personal information, including internet activity on websites not connected to Google."[9]

II. Google Uses Firebase SDK to Surreptitiously Collect Users' Communications with Third-Party Apps

37. Mobile "apps" (shorthand for "applications") are software programs that run on mobile devices (e.g., smart phones, tablets).

38. Throughout the Class Period, the overwhelming majority of apps running on Class members' mobile devices have been third-party apps, meaning apps designed, developed, coded, and released by third-party developers. Google did not own or directly control these third-party developers.

39. Firebase SDK is a suite of software development tools that Google has owned and maintained throughout the Class Period. Firebase SDK is intended for use by third-party software developers, including developers of third-party apps for mobile devices. SDK stands for "software development kit." Google calls Firebase SDK a "comprehensive app development platform." Google states that Firebase SDK allows developers to "build apps fast, without managing infrastructure," and that it is "one platform, with products that work better together."[10]

40. On May 20, 2016, Jason Titus, Vice President of Google's Developer Products Group, stated that more than 450,000 software developers were using Firebase SDK.

41. Throughout the Class Period, Google made significant efforts to coerce app developers to use Firebase SDK. For example:

a. Google requires third-party developers to use Firebase SDK in order to use

---

[9] *Correction: ACCC Alleges Google Misled Consumers About Expanded Use of Personal Data*, AUSTRALIAN COMPETITION & CONSUMER COMM'N (July 27, 2020), https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data#:~:text=The%20ACCC%20has%20launched%20Federal,Google%2C%20including%20for%20targeted%20advertising (last visited Nov. 11, 2020).

[10] *See* FIREBASE, https://firebase.google.com/ (last visited Nov. 11, 2020).

the Google Analytics service to gain information about customers' use of the app;[11]

b. Google requires third-party developers to use Firebase SDK in order to make the app pages searchable on Android devices;

d. Google through Firebase SDK provides support for Google's "Play Store"—a platform on which third-party app developers distribute their app to consumers and process payments in the app.

42. As a result of Google's coercive practices, more than 1.5 million apps currently use Firebase SDK. That includes the vast majority of third-party apps that are currently in use on mobile devices that run Google's Android operating system. The third-party apps utilizing Firebase SDK include, for example, The New York Times, Duolingo, Alibaba, Lyft, Venmo, and The Economist.[12]

43. The Firebase SDK scripts copy and transmit to Google's servers in California many different kinds of user communications between app users on the one hand and, on the other hand, the app and the persons and entities who maintain the app (typically, the app's owners and developers), by overriding device and account level controls.

44. All of these communications qualify as "covered information" for purposes of the 2011 FTC Consent Order, and these communications contain personally identifiable information. These communications contain information relating to: (1) who the user is; (2) where the user is physically located; (3) what content the user has requested from the app (e.g., the app page URL); (4) what content the user has viewed on the app; and (5) much other information relating to the user's interaction with the app.

45. Through the Firebase SDK scripts, Google intercepts these communications while

---

[11] For Android, see *Mobile App Reporting in Google Analytics - Android*, GOOGLE ANALYTICS, https://developers.google.com/analytics/devguides/collection/firebase/android (last visited Nov. 11, 2020) ("App reporting in Google Analytics is natively integrated with Firebase, Google's app developer platform . . . ."). For Apple iOS, see *Mobile App Reporting in Google Analytics - iOS*, GOOGLE ANALYTICS, https://developers.google.com/analytics/devguides/collection/firebase/ios (last visited Nov. 11, 2020) (also stating that "[a]pp reporting in Google Analytics is natively integrated with Firebase, Google's app developer platform . . . .").

[12] FIREBASE, https://firebase.google.com/ (last visited Nov. 11, 2020).

the same are in transit and simultaneously sends surreptitious copies of them to Google even if the user is not engaged with any Google site or functionality; even if the user is not logged in to his or her Google account; and even if the user has "turned off" WAA and/or sWAA. From the apps, the Firebase SDK overrides the mobile device level controls, and causes the device to transmit the intercepted browsing data. Importantly, Google cannot receive this data without overriding device level settings, because the devices ultimately transmit and receive data, sitting between the user using the app, and the app server in the mobile cloud.

46. The Firebase SDK scripts do *not* cause the apps to give any notice to the user that the scripts are surreptitiously copying the communications and sending those copies to Google.

47. These Firebase SDK scripts work on all mobile devices running all the major operating systems—not just the Android system, but also Apple's iOS and many others. Specifically on Android OS, Google surreptitiously collects the app-browsing data through the Android GMS process, overriding device level controls.

48. Here is one example of the kind of communications between users and third-party apps that Google intercepts and copies using the Firebase SDK scripts, even when the user has exercised their privacy controls by turning WAA and/or sWAA off: When a user clicks on an app icon on his or her mobile device, that opens the app and a line of communication between the user, through his or her mobile device, and the app's application server. If the user were to click on the New York Times app, for example, that would open a line of communication with the New York Times' application server to request content to be delivered to the user, such as the most current news of the day. For users who have elected to not allow Google to collect their app-browsing activity by turning off WAA and/or sWAA, Google, by means of the Firebase SDK scripts, surreptitiously intercepts the user's request as the request is in transit to the app's application server, and simultaneously transmits a copy of the request to Google without disclosure to the user or the user's consent.

49. A second example is advertisements delivered by Google on third-party apps. Google offers advertisement services such as Real Time Ad Bidding for which Google, through the Firebase SDK scripts, intercepts and duplicates communications between users and third-party

apps while they are in transit and simultaneously transmits the communications to Google controlled databases. The duplicated communications delivered simultaneously to Google include the user's personal information, from the communication between the user and the third-party apps, such as the mobile app page being requested and the device from which the request is being made. This simultaneous interception and transmission to Google enables Google to target the user with a targeted advertisement in real time. This means that when a user communicates with a third-party app to, for example, request app content related to flat screen televisions, through the process described above, Google will simultaneously intercept the user's communication and use it in real time to earn money by generating and serving the user an advertisement for flat screen televisions, in the third-party app. To accomplish ad delivery in real time, Google must intercept the communication between the user and the third-party app immediately, at the moment the request is sent by the user to the third-party app, so that Google can serve a targeted advisement on the user simultaneously with the requested app content.

50. Google's own documentation states that the Firebase SDK scripts allow Google to "[l]og the user's interactions with the app, including viewing content, creating new content, or sharing content."[13] The Firebase SDK scripts also allow Google to identify certain "actions" that consumers take within an app, such as "viewing a recipe." Thus, for example, Google's Firebase documentation states that Firebase can "log separate calls" each time a consumer "view[s] a recipe (start) and then clos[es] the recipe (end)." (This Google documentation, however, does *not* disclose that these scripts transmit this information and surreptitious copies of the data to Google even when the user switches the "Web & App Activity" feature off. And the documentation certainly does not disclose that Firebase SDK would be used to circumvent device and account level settings.)

51. Firebase SDK uses the term "event" to describe a wide range of user activity with

---

[13] *Log User Actions*, FIREBASE, https://firebase.google.com/docs/app-indexing/android/log-actions (last visited Nov. 11, 2020). Google has taken the position in its Interrogatory responses that Firebase App Indexing does not collect event data unless "Web & App Activity" is switched to "on." Plaintiffs are seeking additional discovery about how the "Web & App Activity" control impacts App Indexing.

an app. For example: when the user views a new screen on the app, that event is called "screen_view."[14] When the user opens a notification sent via the app from the Firebase Cloud Messaging system, that event is called "notification_open." And when the user selects content in the app, that event is called "select_content."

52. The Firebase SDK scripts "automatically" copy and transmit (to Google) communications relating to at least 26 different kinds of events (including "screen_view" and "notification_open," described above), through the users' device. The Firebase SDK scripts will "collect" these events "automatically," meaning, even if the developer does not "write any additional code to collect these events."

53. In addition to the 26 different "automatically collected events," Firebase SDK permits app developers to code their apps to collect information about many more events (including "screen_view," described above). Furthermore, Firebase SDK enables developers to create their own "custom events" to be tracked in their apps.[15] Depending on how the app's code is written, Firebase SDK may also copy and transmit these and many additional events to Google's servers, through the users' device. On Android OS, these intercepted messages are concurrently aggregated and facilitated by a background process called Google Mobile Service (GMS), which aggregates similarly intercepted messages across all the apps using Firebase SDK, so that user identity can be easily tracked across the apps, and so that browsing activity can be immediately associated and correlated for meaningful real-time context.

54. Firebase SDK associates almost every kind of event with one or more specific pieces of information, called "parameters." For example: when the user views a new screen (event: "screen_view"), the Firebase SDK scripts copy and transmit through the device at least seven different parameters to Google including "firebase_screen_id" and "engagement_time_msec."

---

[14] *See Automatically Collected Events*, FIREBASE HELP, https://support.google.com/firebase/answer/6317485?hl=en#:~:text=Automatically%20collected%20events%20%20%20%20Event%20name,currency%2C%20quan%20...%20%2023%20more%20rows%20 (last visited Nov. 11, 2020).

[15] *Google Analytics 4 Properties Tag and Instrumentation Guide*, GOOGLE ANALYTICS, https://developers.google.com/analytics/devguides/collection/ga4/tag-guide (last visited Nov. 11, 2020).

When the user opens a notification (event: "notification_open"), then the Firebase SDK scripts copy and transmit at least seven parameters to Google including "message_name," "message_time," "message_id," "topic," and "label." And when the user selects content in the app (event: "select_content"), then the Firebase SDK scripts copy and transmits through the device at least two parameters: "content_type" and "item_id."

55. The Firebase SDK scripts "automatically" copy and transmit five basic "parameters" about all events. These five automatically transmitted parameters are: "language"; "page_location"; "page_referrer"; "page_title"; and "screen_resolution."[16] According to Google, these five parameters are "collected by default with every event." This means that every time the user interacts with an app (in any sort of event), Firebase records that interaction by copying and transmitting to Google's servers through the device at least those five parameters.

56. Focusing just on the three of the five "parameters" that Google "automatically" transmits: the "page_title" parameter informs Google what the user is viewing; the "page_referrer" parameter informs Google whether the user arrived at that page from another place where Google has a tracker (and if so, the identity of that other place); and the "page_location" parameter informs Google of the URL address (e.g., internet address) of the content the user is viewing on his or her device.

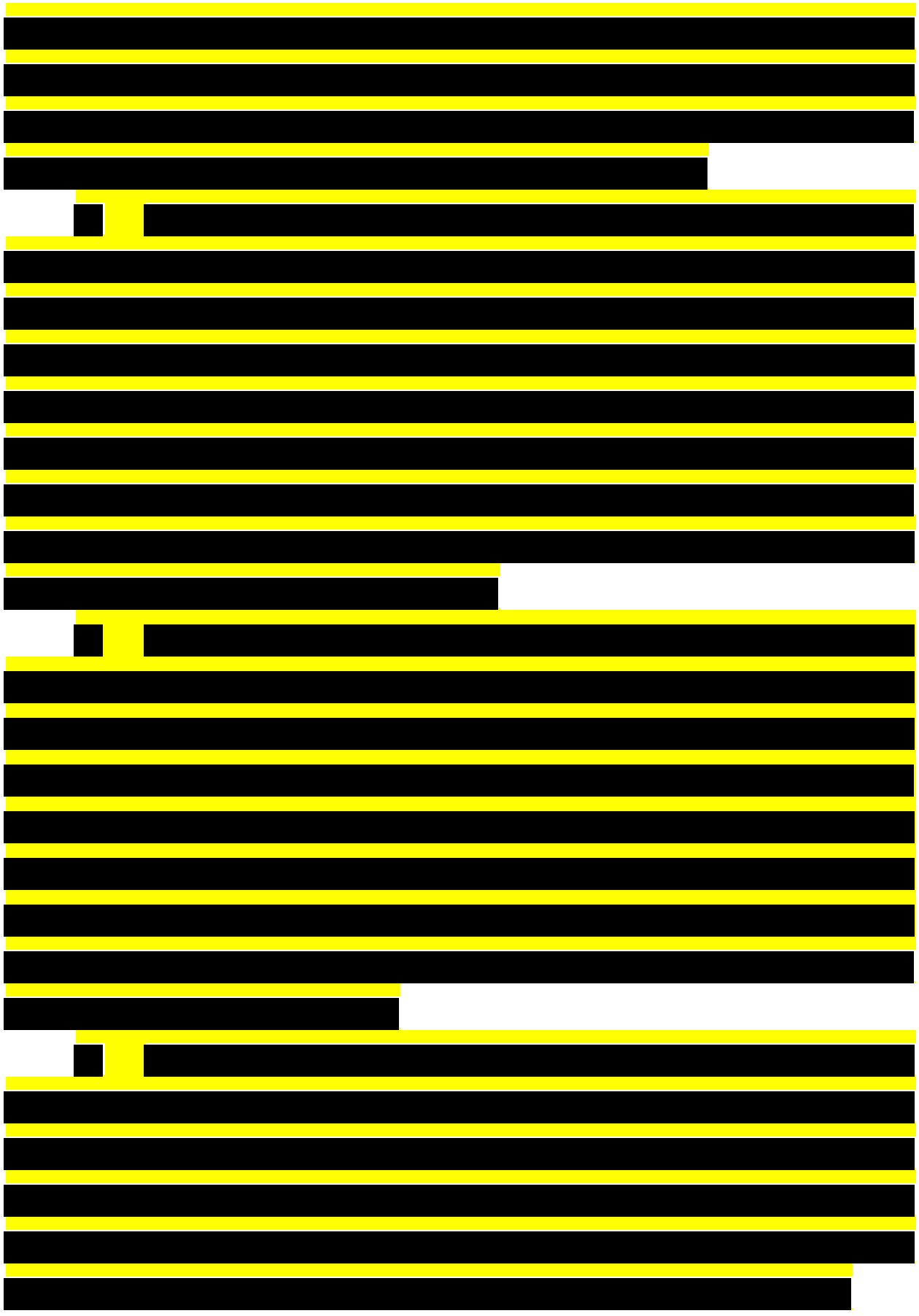
57. Google does not notify its users of these Firebase SDK scripts and how Google actually uses them, which cause the copying and duplication of browsing data to be sent to Google, for at least Google Analytics for Firebase, AdMob, and Cloud Messaging for Firebase. These scripts are hidden from users and run without any notice to users of the interception and data collection even when they exercise their device level controls, which exceeds all contemplated and authorized use of the users' data. All of these Firebase SDK products surreptitiously provide app browsing data to Google on mobile devices, overriding their device level controls, including

[16] *Automatically Collected Events*, FIREBASE HELP, https://support.google.com/firebase/answer/6317485?hl=en#:~:text=Automatically%20collected%20events%20%20%20%20Event%20name,currency%2C%20quan%20...%20%2023%20more%20rows%20 (last visited Nov. 11, 2020).

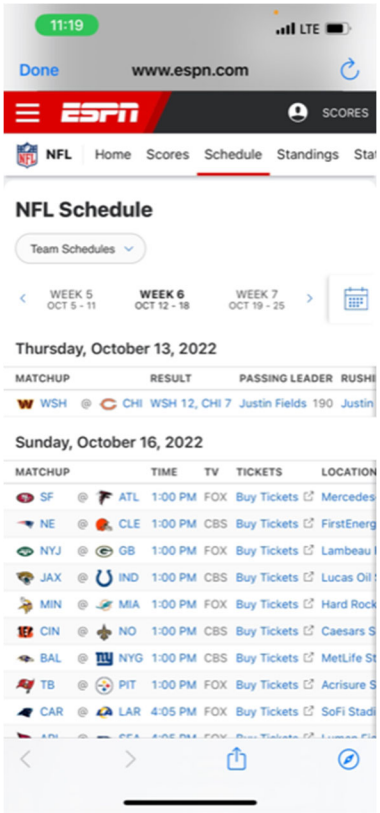
through background processes such as Android GMS.

58. Users have no way to remove these Firebase SDK scripts or to opt-out of this data collection. Google intentionally designed these scripts in such a way as to render ineffective any barriers users may attempt to use to prevent access to their information, including by turning off the "Web & App Activity" feature.

III. Through Discovery and Google's Representations in this Case, Plaintiffs Begin to Understand that [redacted]



[redacted]

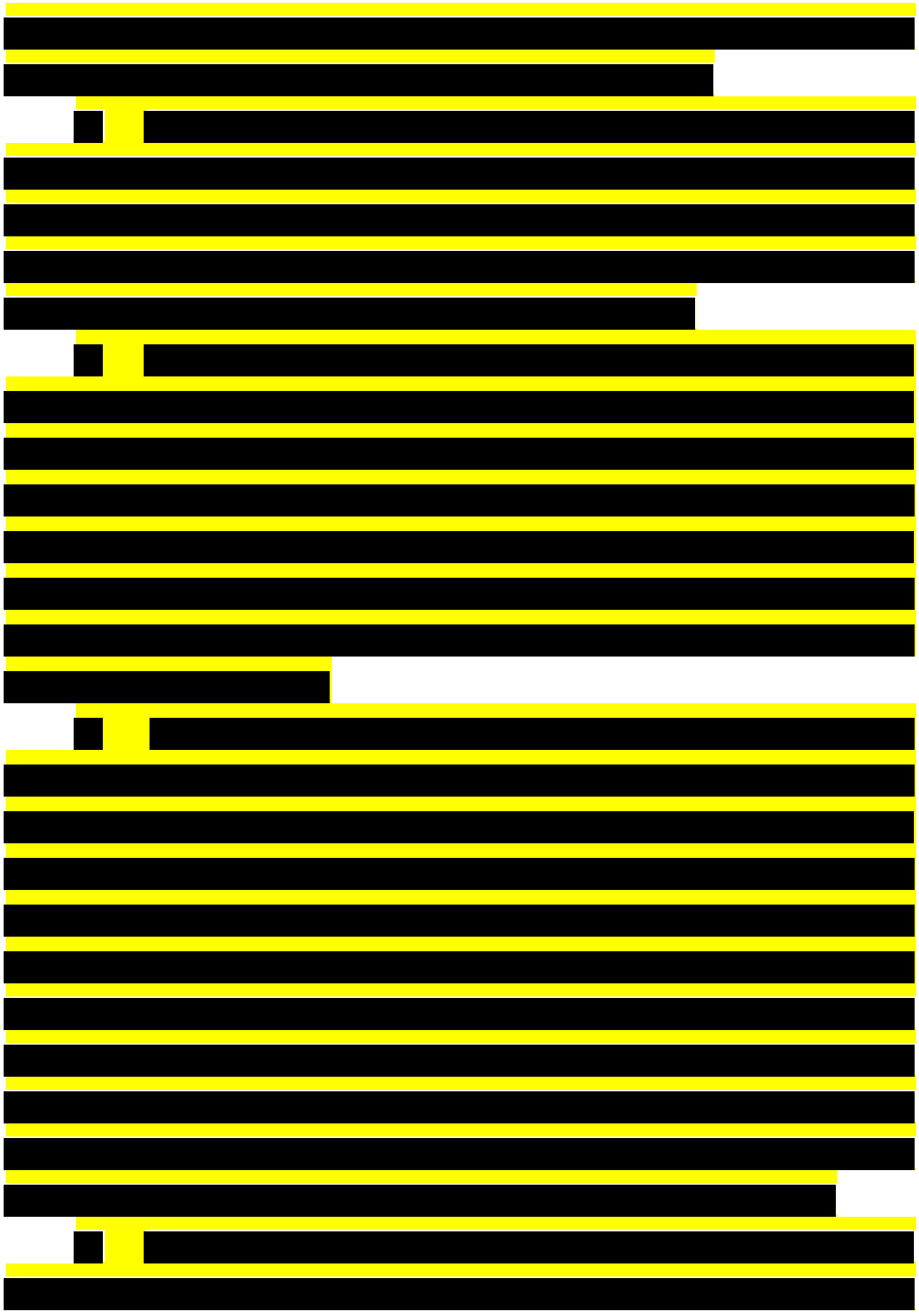


[redacted]

[redacted]

IV. Through Discovery and Google's Representations in this Case, Plaintiffs Now Are Starting to Understand that Google Also Saves Activity Information Related to Users' Interactions with [redacted] When WAA and/or sWAA Are Off

[redacted]



V. Users Turned off the "Web & App Activity" and/or "Supplemental Web & App Activity" Feature to Prevent Google from Collecting and Saving Their Data, but Google Continued Without Disclosure or Consent to Intercept and Save Those Communications

A. Google's "Web & App Activity" Feature

80. In or before 2015, Google launched the "Web & App Activity" feature.

81. Throughout the Class Period, users have been able to access the "Web & App Activity" feature in at least two ways: through Google's website, and through the "Settings" menu of a mobile device running Android OS. Google presented such settings to their business partners as device level controls, including by requiring the controls and accompanying representations written by Google as part of the Android OS, as licensed to Android device manufacturers, such as Samsung.

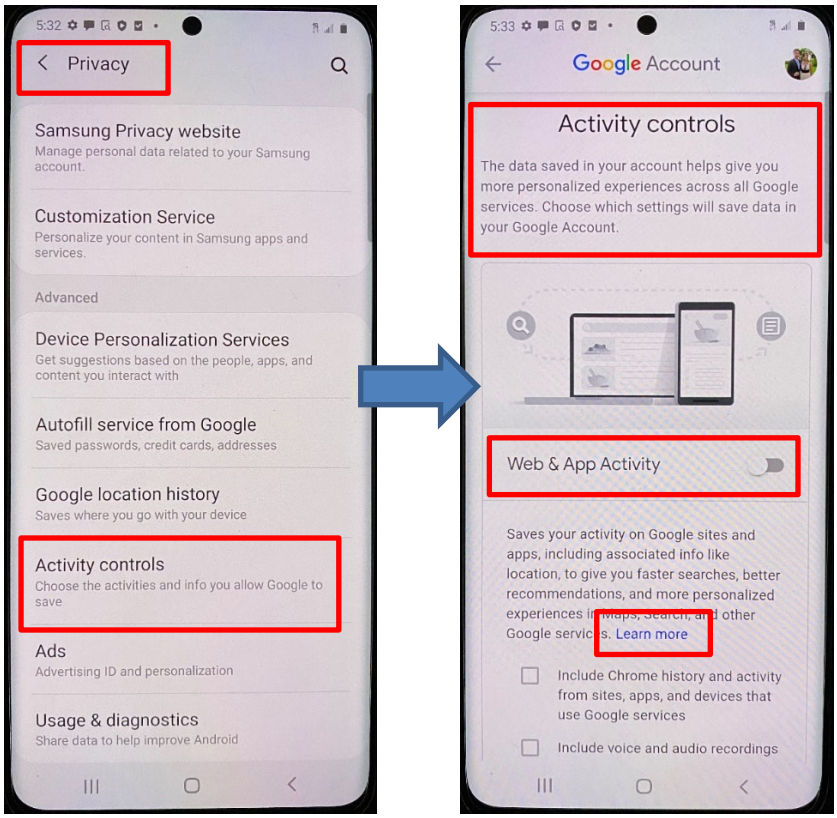
82. To access the "Web & Activity" feature through Google's website, a user would direct his or her web browser to Google's My Activity website (and previously Google's My

Account website), and would then log on with their Google account credentials. The first screen of the My Activity website displays, among other options, the "Web & App Activity" feature. By clicking on the words "Web & App Activity," the user is taken to a second screen, which displays the image of a switch beside the words "Web & App Activity." The user can then toggle the switch "off" to turn off the "Web & App Activity" feature.[17]

83. To access the "Web & Activity" feature through a mobile device running Google's Android operating system, the user would use the phone's "Settings" application.[18] For example, on a Samsung phone running the Android system, the "Settings" application includes a section entitled "Privacy Controls." (Shown in "Screen 1," below.) Within that "Privacy Controls" menu, the user can select "Activity Controls" to "Choose the activities and info you allow Google to save," which would open a new screen. (Shown in "Screen 2," below.) In that second "Activity Controls" screen, the phone displays the image of a switch beside the words "Web & App Activity." The user can then toggle the switch "off" to turn off the "Web & App Activity" feature.

[17] Google previously offered the option to "pause" Web & App Activity. "Pausing" this feature likewise did not stop the Google interception, data collection, and use at issue in this lawsuit.

[18] The images for this paragraph were captured in July 2020, during the filing of the initial Complaint. Since then, Google has changed the language of the device level settings on Android phones, including the Samsung phones referenced herein. The reasons why Google removed such language, and its communications with manufacturers such as Samsung, will be subject to discovery.



SCREEN 1[19] SCREEN 2

84. Beneath the "Web & App Activity" control switch, there is a separate box that the user may click to allow Google to "Include Chrome history and activity from sites, apps, and devices that use Google services." Users who access "Web & App Activity" through the Google website are likewise presented with this separate box. When the "Web & App Activity" switch is turned off, either through the Google website or Android "Settings" application, the box that states "Include Chrome history and activity from sites, apps, and devices that use Google services" is also automatically turned off and cannot be toggled to on. This separate box is known as "supplemental Web & App Activity" or sWAA. [redacted] A user can elect to turn on WAA but turn off sWAA and/or keep sWAA off.

85. The Google Privacy Policy also defines "Google services" to include Google apps and sites as well as Google products integrated into third-party apps and sites, such as Firebase

[19] The highlighted language from this screen is part of the OS language written by Google.

SDK products like Google Analytics for Firebase, AdMob, and Cloud Messaging, [redacted] [20] Ex. A (Google Privacy Policy) at 2.

86. Google simultaneously tracks the user's setting of the WAA and sWAA features (whether "on" or "off") across all Google's services and devices in real time. Thus, if a user turns off WAA and/or sWAA in the user's phone, then that change will also be reflected when the user logs on to Google's "My Activity" website using the user's laptop. Similarly, if a user then uses the laptop to turn WAA or sWAA back "on," using the "My Activity" website, then that feature will also be turned "on" in the user's Android phone "Settings" application.

87. However, contrary to Google's disclosures (described below), turning off the WAA and/or sWAA features actually does nothing to stop Google from receiving, collecting, and using the data transmitted to Google by way of [redacted], including Firebase scripts. Nor does turning off WAA prevent Google from logging, storing, and using information related to users' interactions with [redacted]

B. Google's Privacy Policy and "Learn More" Disclosures Stated That the "Web & App Activity" and "Supplemental Web & App Activity" Features Stops Google from "Saving" Users' Data

88. Throughout the Class Period, Google stated that turning "off" the "Web & App Activity" feature would prevent Google from collecting and saving users' data, including users' communications made via apps. Google's statements appeared in at least four places: Google's "Privacy Policy"; Google's "Privacy and Security Principles"; the "Web & App Activity" feature itself; and Google's "Learn More" disclosures relating to the "Web & App Activity" feature.

1. Google's "Privacy Policy" and "Privacy and Security Principles" Stated That Users Could "Control" What Google Collects

89. Throughout the Class Period, Google's Privacy Policy has defined "Google services" to include "Google apps [and] sites" as well as [redacted] that, like Firebase SDK, are "integrated into third-party apps." The first page of Google's Privacy Policy states:

---

[20] *Google Privacy Policy*, GOOGLE PRIVACY & TERMS (July 1, 2020), https://policies.google.com/privacy/archive/20200701?hl=en-US (last visited Oct. 11, 2022).

> Our ***services include: Google apps, sites*** . . . [and] ***Products that are integrated into third-party apps*** and sites, like ads and embedded Google Maps

Ex. A at 1 (Privacy Policy).

90. From at least May 25, 2018, to the present, Google's Privacy Policy has promised users that "***across our services***, ***you*** can adjust your privacy settings to ***control what we collect and how your information is used***." *Id.* (emphasis added).[21] Earlier versions of Google's Privacy Policy included similar representations.[22]

91. Throughout the Class Period, Google's Privacy Policy has told users that they can "control data" by using Google's "My Activity" website. (As described above, "My Activity" is the website that users can access in order to switch WAA and/or sWAA off.) The Privacy Policy states: "My Activity allows ***you to*** review and ***control data that's created when you use Google services*** . . . ." Ex. A at 9 (Privacy Policy) (emphasis added).

92. Google also stated in its "Privacy and Security Principles," displayed on its "Safety Center" website,[23] that Google would: "[r]espect our users" and "their privacy"; "[b]e clear about what data we collect"; "make it easy to understand what data we collect"; and "[m]ake it easy for people to control their privacy." Google further stated, in these Privacy and Security Principles: "Every Google Account is built with on/off data controls, so our users can choose the privacy

---

[21] *See* Privacy Policy, GOOGLE PRIVACY & TERMS, https://policies.google.com/privacy (last visited Nov. 11, 2020). Google included this same statement—"you can adjust your privacy settings to control what we collect and how your information is used"—in versions of its Privacy Policy dated May 25, 2018, January 22, 2019, October 15, 2019, December 19, 2019, March 31, 2020, July 1, 2020, August 28, 2020, and September 30, 2020. *Id.*

[22] The Google Privacy Policies effective between August 19, 2015 and May 24, 2018 included a section titled "Transparency and choice." That section states that Google's "goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used" and directs users to "[r]eview and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like saved with your account when you use Google services." Also included in the "Transparency and choice" section is the statement that users can "[c]ontrol who you share information with through your Google Account." *See* Aug. 19, 2015 Google Privacy Policy; Mar. 25, 2016 Google Privacy Policy; June 28, 2016 Google Privacy Policy; Aug. 29, 2016 Google Privacy Policy; Mar. 1, 2017 Google Privacy Policy; Apr. 17, 2017 Google Privacy Policy; Oct. 2, 2017 Google Privacy Policy; Dec. 18, 2017 Google Privacy Policy (this policy was effective until May 24, 2018).

[23] *Our Privacy and Security Principles*, GOOGLE SAFETY CENTER, https://safety.google/principles/ (last visited Nov. 11, 2020).

settings that are right for them." Google promised to "ensur[e] that privacy is always an individual choice that belongs to the user." These "principles" have been part of Google's successful efforts to lull users, app developers, and others into a false sense of user control and privacy.

93. Finally, Google's Privacy Policy has stated, throughout the Class Period, that "We will not reduce your rights under this Privacy Policy without your explicit consent."

2. Google's "Web & App Activity" and "Supplemental Web & App Activity" Features and Google's "Learn More" Disclosures with Respect to "Web & App Activity" Explained That Turning the Feature off Would Prevent Google from Saving Information Related to [redacted] and Third Party Apps

94. As described above, Google's "My Activity" website is one of two ways users can switch off "Web & App Activity." By clicking on the words "Web & App Activity" on the "My Activity" website, the user is taken to a second screen, which displays the image of a switch beside the words "Web & App Activity." On that screen, Google states that "Web & App Activity" provides "control" that includes "activity on Google sites and apps" and "activity from sites, apps, and devices that use Google services."

95. The "My Activity" website also contains a hyperlink with the words "Learn more," located below the on/off switch for "Web & App Activity." When users click on this "Learn more" hyperlink, their browser then displays a new webpage entitled "Find & Control your Web & App Activity."[24] On that page, during the Class Period, Google made the following disclosures:

> **SEE & CONTROL YOUR WEB & APP ACTIVITY**
>
> . . . .
>
> You can turn Web & App Activity off or delete past activity at any time…
>
> **I. What's saved as Web & App Activity…**
>
> Info about your searches and other activity on Google sites, apps, and services
>
> When Web & App Activity is on, Google saves information like:

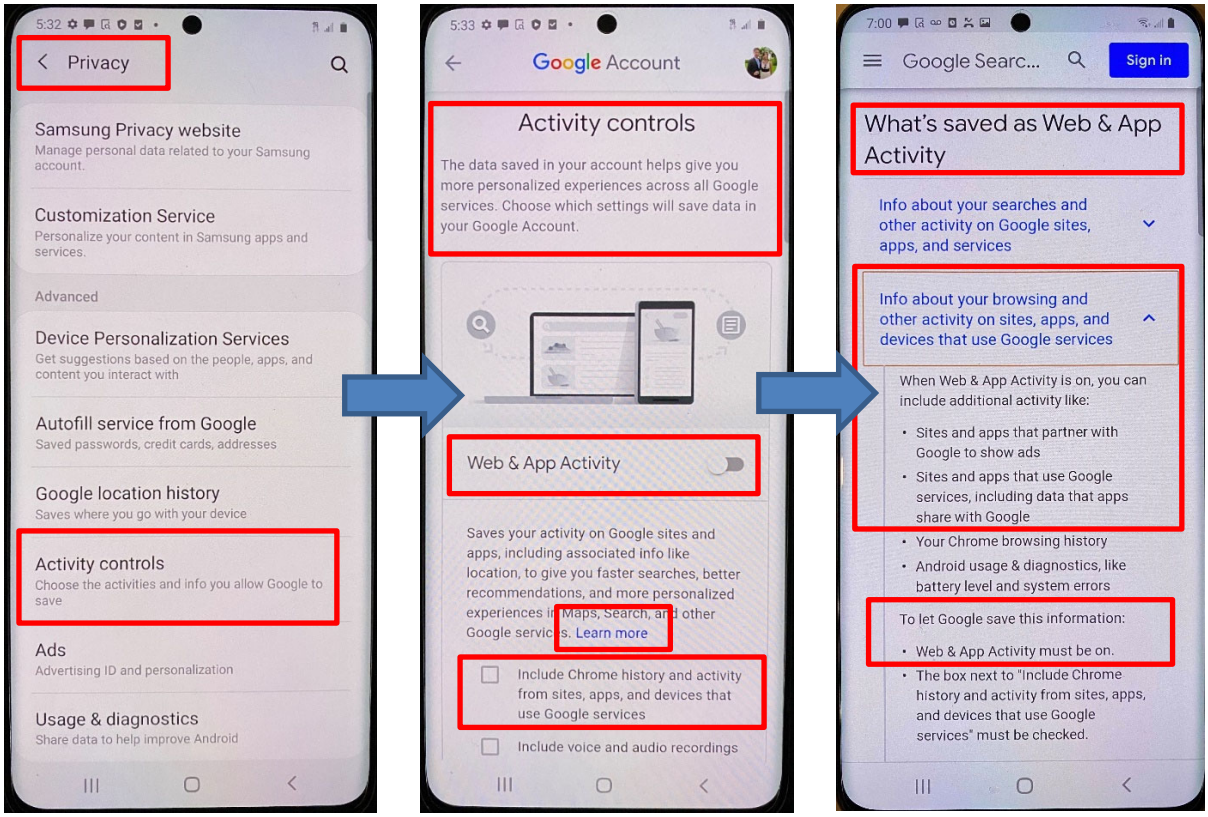
[24] *Find & Control Your Web & App Activity*, GOOGLE SEARCH HELP, https://support.google.com/websearch/answer/54068?visit_id=637255508625725742210537612 8&hl=en&rd=1 (last visited Nov. 11, 2020).

> - Searches and other things you do on Google products and services, like Maps and Play
> - Your location, language, IP address, referrer, and whether you use a browser or an app
> - Ads you click, or things you buy on an advertiser's site
> - Information on your device like recent apps or contact names you searches for
>
> . . .
>
> Info about your browsing and other activity on sites, apps, and devices that use Google services
>
> When Web & App Activity is on, you can include additional activity like:
>
> - Sites and apps that partner with Google to show ads
> - Sites and apps that use Google services, including data that apps share with Google
> - Your Chrome browsing history
> - Android usage & diagnostics, like battery level and system errors
>
> ***To let Google save this information:***
>
> - ***Web & App Activity must be on***.
> - The box next to "Include Chrome history and activity from sites, apps, and devices that use Google services" must be checked.

Id. (emphases added). This is a plain and direct statement to users that the switch for "Web & App Activity" "must be on" "[t]o let Google save this information," including "searches and other things you do on ***Google products***" as well as "[i]nfo about" the users' "activity on sites, ***apps***, and devices ***that use Google services***." *Id.* "Google services" includes, of course, Firebase SDK, Google Analytics for Firebase, [redacted] Google's own Privacy Policy defines the term "Google service" to include these [redacted] embedded in non-Google apps. Ex. A (Privacy Policy) at 1 ("Our ***services include:*** . . . ***products that are integrated into third-party apps*** . . . .").

96. Google's "Learn More" disclosures on the Android "settings" screens also stated that turning the Web & App Activity feature off would prevent Google from "sav[ing]" information related to [redacted] and third-party apps. As described above, users with devices running Google's Android operating system have an additional means of switching the "Web & App Activity" feature off—namely, they can do this using the "Activity Controls" section of the

"Privacy" menu within these devices' "Settings" application. *Supra*, ¶ 83. This section also contains a "Learn more" hyperlink (see bottom of Screen 2, below) which, if selected, opens a web browser application on the device and displays to the user the same webpage, entitled "See & Control your Web & App Activity," within Google's "My Activity" website. *Supra*, ¶ 95 (describing and quoting this webpage). (Screen 3, below, shows a screenshot of part of this webpage as displayed on the device.)



SCREEN 1 SCREEN 2 SCREEN 3

97. In Screen 1, the user is promised that the "Activity controls" will enable the user to "[c]hoose the activities and info you allow Google to save."

98. Screen 2 makes clear that this "info" includes both "activity on Google sites and apps" as well as "activity from sites, apps, and devices that use Google services" and that "Web & App Activity" (including sWAA) is the relevant control.

99. In Screen 3, after selecting "Learn more," the user is told that "To let Google save this information: Web & App Activity must be on."

100. Thus, users who used their Android "Settings" application to learn more about the

"Web & App Activity" feature received the same misleading disclosures as did users who visited the "My Activity" website.

101. Thus, Google publicly admits that its Activity Controls, including "Web & App Activity," are supposed to "allow you to switch the collection and use of data on or off."

102. Based on Google's disclosures described and quoted above, Plaintiffs and Class members had the objectively reasonable belief that Google would stop collecting their communications and other interactions with apps on their phones—"across [Google's] services"—if the users turned the WAA and/or sWAA switch to "off." [redacted]

103. Plaintiffs and Class members could not possibly have consented to Google's collection of their communications and other interactions with apps on their mobile devices when they turned the "Web & App Activity" switch to off. [redacted]

3. Google Knew That Its Disclosures Led Users to Believe That Turning "Web & App Activity" off Would Prevent Google from Collecting Communications with Apps, and Saving Information Related to Their Interactions with [redacted]

104. As a result of the Arizona Attorney General's investigation (*see supra*, ¶¶ 33-35), several heavily redacted internal Google documents have been made public. These documents refer to Google's "Web & App Activity" feature and its on/off switch. The documents indicate that Google's own employees understood that Google's disclosures to consumers, regarding this switch, misled consumers into believing, wrongly, that turning the switch "off" would prevent [redacted]

For example:

a. On February 2, 2017, one Google employee (name redacted by Google for privacy reasons) referenced "work in progress" at Google "trying to rein in the overall mess that we have with regards to data collection, consent, and storage." This was in response to another

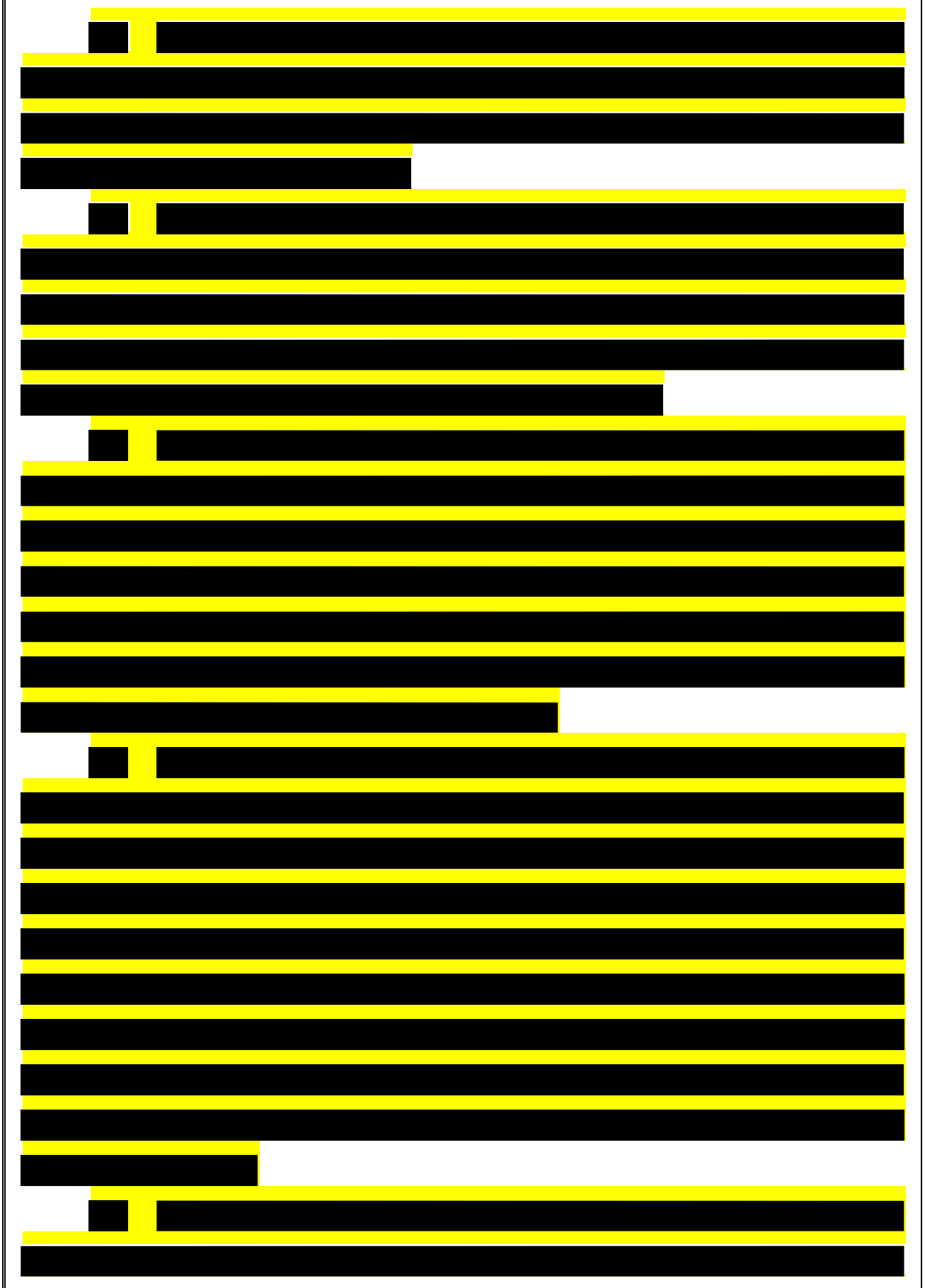
Google employee (name redacted by Google for privacy reasons), asking a question regarding whether "users with significant privacy concerns understand what data we are saving?" Another Google employee (name redacted by Google for privacy reasons) stated that this area was "super messy" and users needed to "make sense out of this mess." The "overall mess" with Google's data collection and consent described in these documents includes the Web & App Activity feature.

b. On August 13, 2018, one Google employee (name redacted by Google for privacy reasons) referenced "Web/App Activity" and commented that the "current UI [user interface] feels like it is designed to make things possible, yet difficult enough that people won't figure it out." The Google employee also noted that selections were "defaulted to on, silently appearing in setting menus you may never see is <redacted>." These internal Google comments specifically addressed Web & App Activity, characterizing Web & App Activity as something "difficult enough" that users "won't figure it out."

c. On August 14, 2018, one Google employee (name redacted by Google for privacy reasons) referenced Web & App Activity, stating "I did not know Web and App activity had anything to do with location. And seems like we are not good at explaining this to users." Another Google employee (name redacted by Google for privacy reasons) added: "Definitely confusing from a user point of view if we need googlers [to] explain it to us[.]" Google employees recognized Google was "not good" (perhaps intentionally so) at explaining the Web & App Activity feature.

d. One heavily redacted 2017 Google presentation concerns a study that specifically focused, at least in part, on "Consent" and asked, "Do users comprehend what will happen if they turn on the Web & App activity setting . . . ." The presentation includes a lengthy, but mostly redacted, section of "Detailed findings." Those findings state that "Participants had difficulty [redacted]" and that the "effect of the activity of the Web & App Activity [redacted]."

105. On information and belief, unredacted versions of those documents and other internal Google documents will further confirm that not even Google believes its users had consented to Google's interceptions between users and apps when "Web & App Activity" was switched off.



[redacted]

4. Google's Passing Reference to "Your Google Account" Does Not Constitute Consent

111. During the Class Period, Google made much of its commitment to privacy. For example, Google's CEO promised consumers, in a *New York Times* op-ed, that "[t]o make privacy real, we give you clear, meaningful choices around your data."[25]

112. Now faced with this lawsuit compelling it to honor these claims, Google has abandoned this commitment to clear and meaningful choices, instead contending that its Privacy Policy and promises were a ruse.

113. Google's first motion to dismiss contended—incorrectly and incredibly—that the "Learn more" disclosures described above somehow told users that Google would continue to intercept, copy, collect and save their communications with apps, even when the "Web & App Activity" feature was turned "off." Google's motion relied on the words "saved in your Google Account," taken from a single sentence in the "See & Control your Web & App Activity" page:

> If Web & App Activity is turned on, your searches and activity from other Google services are ***saved in your Google Account***, so you may get more personalized experiences, like faster searches and more helpful app and content recommendations.

Google argued that the words "saved in your Google Account" conveyed to users that the "Web & App Activity" on/off switch was meaningless—that it would not do precisely what Google's Privacy Policy (and the rest of the "Learn More" hyperlinked page) says that the switch would do. Rather, these five words, according to Google, indicate that the "off" switch has all the effect of a light switch during a blackout: The switch merely toggles off what data Google will *display for the user* in the user's "account." To state this contention plainly reveals how outlandish it is. Over and over again Google's Privacy Policy and "Learn more" disclosures told users that the "Web & App Activity" feature switch would "control" what "Google saves"; "what we collect"; and "how

[25] Sundair Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, THE NEW YORK TIMES (May 7, 2019), *available at* https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html (last visited Nov. 11, 2020).

your information is used"—across "Google services." The five words highlighted by Google do nothing to diminish Google's promises.

114. Google's reliance on these five words is particularly troubling because Google itself, in many other disclosures, told users that Google promised to "Be clear about what data we collect and why. To help people make informed decisions about how they use Google products, we make it easy to understand what data we collect, how it's used, and why. Being transparent means making this information readily available, understandable, and actionable."[26] *See infra*, ¶¶ 117-35 (collecting such public statements by Google). Google's made-for-litigation argument, relying on a passing reference to "activity" being "saved in your Google account," is not the kind of "easy to understand" and "transparent" disclosure Google elsewhere promised to its users.

115. Google's argument is wrong for another reason, too: This sentence refers only to what happens if "Web & App Activity ***is turned on.***" Nothing in this sentence limits Google's repeated promises, quoted above, about what would happen when users turned Web & App Activity ***off***. Plaintiffs and the Class members were never told about and were harmed by Google's continued interceptions and collections of data during the times when they turned the switch ***off***.

116. Critically, nowhere in any disclosures did Google ever state that it would continue to collect users' communications with apps when the WAA or sWAA features were turned off. Nor did Google ever state that it would continue to save information about users' interactions with [redacted] when the WAA or sWAA features were turned off. The notion that users and apps consented to this practice is absurd—one cannot consent to what one does not know.

C. Google Obscured Its Collection of These Communications Without Consent Through Its "Pro-Privacy" Campaigns and Other Public Statements

117. In addition to the Privacy Policy and "Learn More" disclosures, described above, Google masked its unauthorized data collection practices (including specifically Google's practice of (1) receiving, collecting, and saving the Firebase SDK [redacted] transmissions while users had switched off the WAA and/or sWAA features and

[26] *Our Privacy and Security Principles*, Google Safety Center, https://safety.google/principles/ (last visited Nov. 11, 2020).

(2) saving information related to users' interactions with [redacted]) through various "pro-privacy" campaigns and other public statements.

118. On June 1, 2015, Google Product Manager of Account Controls and Settings, Guemmy Kim, published an article titled "Keeping your personal information private and safe—and putting you in control."[27] The article states that "Google builds simple, powerful privacy and security tools that keep your information safe and put you in control of it," such as the "new hub" called "My Account" (which at that time included the Web & App Activity feature that is at issue in this lawsuit). This article told users that "My Account gives you quick access to the settings and tools that help you safeguard your data, protect your privacy, and decide what information is used to make Google services work better for you." The article stated that users can "[m]anage the information" that Google "use[s]" from Google "products." As an example of how users can control how Google uses their information, the article further represented that "you can turn on and off settings such as Web and App Activity."

119. On June 1, 2016, Kim published another article titled "Celebrating My Account's first birthday with improvements and new controls." This article described Google's My Account hub (which at that time included the Web & App Activity feature at issue in this lawsuit) as "a hub that gives you quick access to controls for safeguarding your data and protecting your privacy on Google."[28] The article touted how Google's tools "make it easy for you to control your privacy" and represented that when "you entrust your data to Google, you should expect powerful security and privacy controls."

120. On September 8, 2017, Google Product Manager Greg Fair published an article titled "Improving our privacy controls with a new Google Dashboard" in which he touted how Google has "[p]owerful privacy controls that work for you" and emphasized that users had

---

[27] Guemmy Kim, *Keeping Your Personal Information Private and Safe—and Putting You in Control*, GOOGLE, THE KEYWORD (June 1, 2015), *available at* https://blog.google/topics/safety-security/privacy-security-tools-improvements/ (last visited Nov. 11, 2020).

[28] Guemmy Kim, *Celebrating My Account's First Birthday with Improvements and New Controls*, GOOGLE, THE KEYWORD (June 1, 2016), *available at* https://blog.google/technology/safety-security/celebrating-my-accounts-first-birthday/ (last visited Nov. 11, 2020).

"control" over their information and tools "for controlling your data across Google."[29] Mr. Fair specifically referenced the My Activity hub (formerly named "My Account"), which at that time included the Web & App Activity feature at issue in this lawsuit. Mr. Fair stated: "You–and only you–can view and control the information in My Activity." After describing this privacy control, Mr. Fair boasted Google's efforts in "[b]uilding tools that help people understand the data stored with their Google Account and control their privacy."

121. On June 21, 2018, Google Product Manager, Jan Hannemann, published an article titled "More transparency and control in your Google Account" in which he wrote: "For years, we've built and refined tools to help you easily understand, protect, and control your information. As needs around security and privacy evolve, we will continue to improve these important tools to help you control how Google works for you."[30]

122. On May 7, 2019, Google CEO Pichai published an op-ed in the *New York Times*, titled "Privacy Should Not Be a Luxury Good," in which he stated that: "we [at Google] care just as much about the experience on low-cost phones in countries starting to come online as we do about the experience on high-end phones. Our mission compels us to take the same approach to privacy. For us, that means privacy cannot be a luxury good offered only to people who can afford to buy premium products and services."[31] Mr. Pichai further stated that it is "vital for companies to give people clear, individual choices around how their data is used" and that Google focuses on "features that make privacy a reality — for everyone." He continued: "To make privacy real, we give you clear, meaningful choices around your data."[32]

123. On the same date, May 7, 2019, Google CEO Pichai gave the keynote address at Google's 2019 I/O developer conference. He stated: "[a]nother way we build for everyone is by

---

[29] Greg Fair, *Improving Our Privacy Controls with a New Google Dashboard*, GOOGLE, THE KEYWORD (Sept. 8, 2017), https://www.blog.google/topics/safety-security/improving-our-privacy-controls-new-google-dashboard/ (last visited Nov. 11, 2020).
[30] Jan Hannemann, *More Transparency and Control in Your Google Account*, GOOGLE, THE KEYWORD (June 21, 2018), https://blog.google/technology/safety-security/more-transparency-and-control-your-google-account/ (last visited Nov. 11, 2020).
[31] Sundar Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, THE NEW YORK TIMES (May 7, 2020), *available at* https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html (last visited Nov. 11, 2020).
[32] *Id.*

ensuring that our products are safe and private, and that people have clear, meaningful choices around their data. We strongly believe that privacy and security are for everyone, not just a few." The full text of his remarks was later published online.[33] Mr. Pichai further stated that Google's "products" are "built on a foundation of user trust and privacy." He represented that Google "ensur[es] that our products are safe and private, and that people have clear, meaningful choices around their data."[34] Recognizing that "privacy and security are for everyone," he also stated: "This is why powerful privacy features and controls have always been built into Google services." Mr. Pichai specifically referenced the Web & App Activity control at issue in this lawsuit, touting how Google was launching the auto-delete functionality as an example of how users can access "privacy controls" to "easily change your privacy settings."

124. In August 2019 Google launched a "pro-privacy" campaign called "Privacy Sandbox." In this campaign, Google promotes itself as a champion of privacy and choice that scrupulously respects the privacy of its users and is transparent about the data it collects.[35] The blog post announcing this initiative declared to users that "Privacy is paramount to us, in everything we do."

125. Since the Privacy Sandbox campaign, Google has indicated that it will require rival adtech companies using Google targeted advertising products to have their own consent directly from the consumers, if the rival adtech companies are to track consumers directly. In response to questions from regulators—such as those in the United Kingdom—regarding whether Google was engaged in anticompetitive conduct, Google responded by indicating that it was protecting consumer privacy.

126. On October 2, 2019, Google Director of Product Management, Privacy, and Data Protection Office, Eric Miraglia, published an article titled "Keeping privacy and security simple,

---

[33] Pangambam S., *Sundar Pichai at Google I/O 2019 Keynote (Full Transcript)*, THE SINGJU POST (June 13, 2019), *available at* https://singjupost.com/sundar-pichai-at-google-i-o-2019-keynote-full-transcript/?singlepage=1.

[34] *Id.*

[35] Justin Schuh, *Building a More Private Web*, Google, The Keyword (Aug. 22, 2019), *available at* https://www.blog.google/products/chrome/building-a-more-private-web/ (last visited Nov. 11, 2020).

for you" in which he represented that when it comes to "privacy and security," "managing your data should be just as easy as making a restaurant reservation."[36] He emphasized how Google was "rolling out more ways for you to protect your data . . . ." He referenced Web & App Activity, stating that Google was allowing users to "automatically delete your Location History and Web & App Activity, which includes things you've searched for and browsed."

127. On December 19, 2019, Google Vice President of Product Privacy Rahul Roy-Chowdhury published an article titled "Putting you in control: our work in privacy this year" in which he represented that Google Account (which includes the Web & App Activity control at issue in this lawsuit) is a "tool[] for users to access, manage and delete their data" and that Google "let[s] you control how your information is used."[37]

128. On January 22, 2020, Google CEO Pichai reiterated that privacy "cannot be a luxury good," and claimed that "privacy" is "at the heart of what we do."[38]

129. On January 28, 2020, Google Vice President of Product Privacy Rahul Roy-Chowdhury published an article titled "Data Privacy Day: seven ways we protect your privacy" in which he identified the Web & App Activity feature and explained how Google's auto-delete functionality would allow users to "choose to have Google automatically and continuously delete your activity and location history after 3 or 18 months. You can also control what data is saved to your account with easy on/off controls in your Google Account, and even delete your data by date, product and topic."[39]

130. On May 7, 2020, Google Director of Product Management, Privacy and Data Protection Office, Eric Miraglia published an article titled "Privacy that works for everyone" in

---

[36] Eric Miraglia, *Keeping Privacy and Security Simple, For You*, GOOGLE, THE KEYWORD (Oct. 2, 2019), *available at* https://blog.google/technology/safety-security/keeping-privacy-and-security-simple-you/ (last visited Nov. 11, 2020).

[37] Rahul Roy-Chowdhury, *Putting You in Control: Our Work in Privacy This Year*, GOOGLE, THE KEYWORD (Dec. 19, 2019), *available at* https://blog.google/technology/safety-security/putting-you-in-control-privacy-2019/ (last visited Nov. 11, 2020).

[38] James Warrington, *Privacy "Cannot Be a Luxury Good," Says Google Boss Under Pichai*, CITY A.M. (Jan. 22, 2020), *available at* https://www.cityam.com/privacy-cannot-be-a-luxury-good-says-google-boss-sundar-pichai/ (last visited Nov. 11, 2020).

[39] Rahul Roy-Chowdhury, *Data Privacy Day: Seven Ways We Protect Your Privacy*, GOOGLE, THE KEYWORD (Jan. 28, 2020), *available at* https://blog.google/technology/safety-security/data-privacy-day-seven-ways-we-protect-your-privacy/ (last visited Nov. 11, 2020).

which he wrote that "you should be able to understand and manage your data–and make privacy choices that are right for you."[40] He referenced the privacy features and controls at issue in this lawsuit, with Web & App Activity, and wrote: "A few years ago, we introduced Google Account to provide a comprehensive view of the information you've shared and saved with Google, and one place to access your privacy and security settings. Simple on/off controls let you decide which activity you want to save to your account" and you "can also choose which activities or categories of information you want to delete." He also touted the "new control" for "Web & App Activity" with the auto-deletion of "your Location History and Web & App Activity data.

131. On June 24, 2020, Google CEO Sundar Pichai published an article titled "Keeping your private information private" in which he represented that "[p]rivacy is at the heart of everything we do" and that Google focuses on "putting you in control" and "working to give you control on your terms."[41] Mr. Pichai specifically referenced Web & App Activity as part of those efforts to treat "your information responsibly" and stated that Google changed its default settings for "new accounts" so that "your activity data will be automatically and continuously deleted after 18 months, rather than kept until you choose to delete it."

132. On or about July 29, 2020, Google submitted written remarks to Congress for testimony by its current CEO Pichai (who helped develop Google's Chrome browser), which stated: "I've always believed that privacy is a universal right and should be available to everyone, and Google is committed to keeping your information safe, treating it responsibly, and putting you in control of what you choose to share."[42]

133. On September 15, 2020, Google's Global Partnership and Corporate Development

---

[40] Eric Miraglia, *Privacy That Works for Everyone*, GOOGLE, THE KEYWORD (May 7, 2019), *available at* https://blog.google/technology/safety-security/privacy-everyone-io/ (last visited Nov. 11, 2020).

[41] Sundar Pichai, *Keeping Your Private Information Private*, GOOGLE, THE KEYWORD (June 24, 2020), *available at* https://blog.google/technology/safety-security/keeping-private-information-private/ (last visited Nov. 11, 2020).

[42] *Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google: Hearing Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, July 29, 2020, https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-PichaiS-20200729.pdf (written testimony of Sundar Pichai, Chief Executive Officer, Alphabet Inc.).

President Donald Harrison stated during a Senate hearing that consent at times "appears confusing" but also represented that users "have control" and that Google wants "our users to be able to make a decision on how they control their data . . . ." He represented that "[u]sers own their data" and that users were "able to make a decision on how they control their data."

134. The statements by Google and its key leaders, described above, were widely publicized to Google users by many different news outlets, which correctly interpreted these statements as claims, by Google, to be safeguarding users' privacy.[43] Google intended these statements to communicate that Google's data-collection practices were more transparent, and more respectful of users' privacy, than were the practices of Google's competitors (e.g., Apple).

135. Google and its key leaders made the statements described above in order to obscure Google's intent to engage in widespread data collection without consent. These statements were intended to convey, and did convey, that Google did not intercept, collect, and save users' data when the users had turned off the "Web & App Activity" feature.

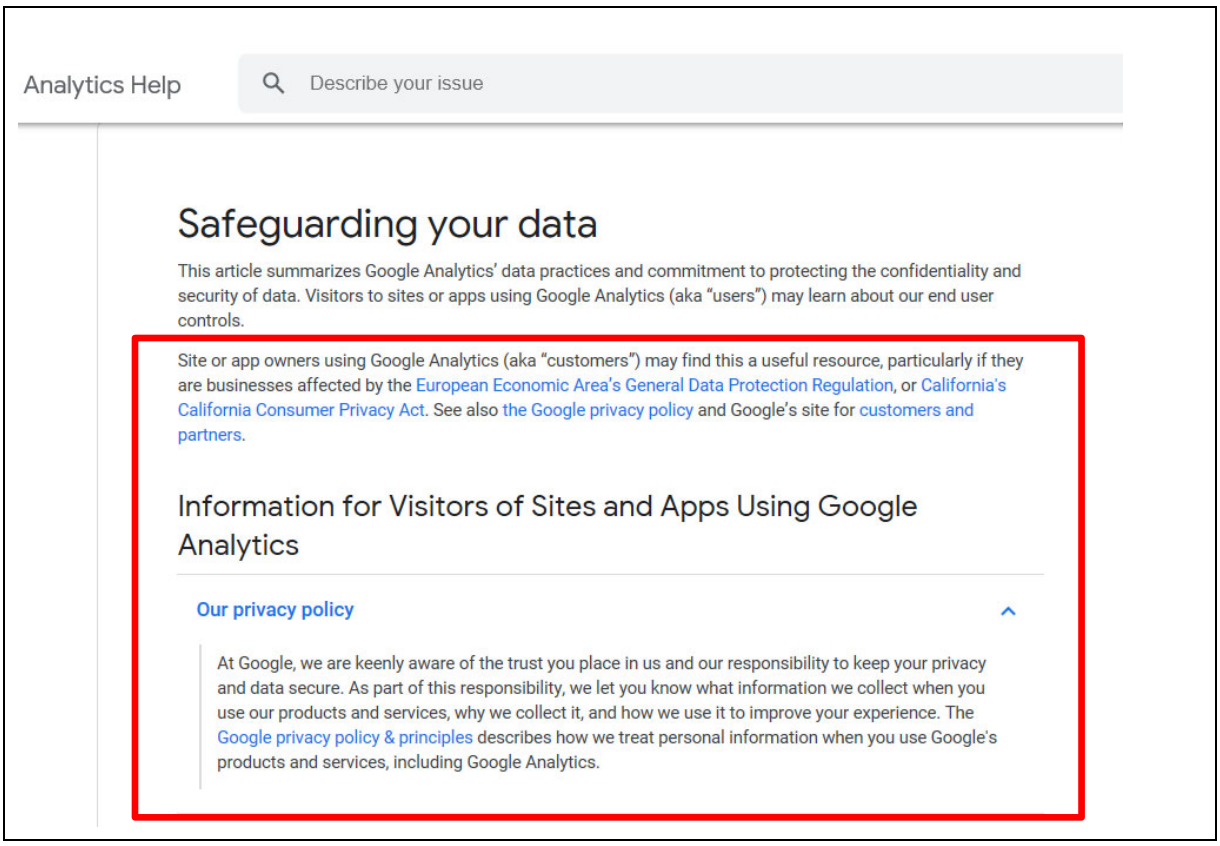
D. Third-Party App Developers Did Not Consent to Google Collecting Users' Communications with Third-Party Apps When "Web & App Activity" Was Turned off

136. Third-party app developers who used [redacted] including Firebase SDK likewise did not consent to Google's interception of users' communications with apps when "Web & App Activity" was turned off. Throughout the Class Period, Google told these developers, in the service agreements, that Google: (1) would comply with its own Privacy Policy; (2) would provide app users with control over their data; and (3) would help the developers to comply with privacy laws and to protect consumers' rights over their data, such as consumers' rights to "access; rectification; restricted processing; [and] portability."

137. Google represented and continues to represent to app developers that Google will adhere to its own Privacy Policy. Specifically, Google states the following, on the Analytics Help

[43] Jon Porter, *Google's Sundar Pichai Snipes at Apple with Privacy Defense*, THE VERGE (May 8, 2019), *available at* https://www.theverge.com/2019/5/8/18536604/google-sundar-pichai-privacy-op-ed-nyt-regulation-apple-cook-advertising-targeting-user-data (last visited Nov. 11, 2020).

page intended for use by app developers who use Firebase SDK:



138. When any app developer clicks on the "Google privacy policy & principles" above, they are taken to Google's Privacy Policy page—the same Privacy Policy page described above. *Supra*, ¶¶ 89-91.[44] In its Privacy Policy, Google falsely stated to its users that "***across our services***, ***you*** [the user] can adjust your privacy settings to ***control what we collect and how your information is used***." As discussed above, Google's Privacy Policy also promises users that Google's "My Activity" website "allows you [the user] to review and control data that's created when you use Google services."

139. Google also gave and gives assurances to app developers in its "Firebase Data Processing And Security Terms" that Google "will protect users' privacy."[45] The purpose of these

---

[44] Google Privacy Policy, GOOGLE PRIVACY & TERMS, https://policies.google.com/privacy?hl=en.

[45] Firebase Data Processing and Security Terms, FIREBASE, https://firebase.google.com/terms/data-processing-terms#9.-data-subject-rights;-data-export (last

(Footnote Continued on Next Page.)

Terms is to give app developers (and regulators, as further discussed below) the assurance that users can limit Google's data collection from Google's "Privacy Controls" as required by recent privacy laws.[46] Such Terms state that "[i]f Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data."[47]$$

140. The California Consumer Privacy Act ("CCPA"), CIPA, the CDAFA, and the FTC Act (as implemented through the FTC Consent Decree) each qualifies as "Non-European Data Protection Legislation."[48] These laws forbid Google from using [redacted] to collect consumers' communications with apps without their consent. Therefore, Google's "Firebase Data Processing And Security Terms" indicated to developers (wrongly) that Google's "Web & App Activity" feature, when turned to "off," would prevent Google from collecting its users' communications with their apps.

141. Accordingly, app developers implementing [redacted] (like Firebase SDK) have not consented, do not consent, and cannot consent to Google's interception and collection of user data for Google's own purposes when users have turned off WAA and/or sWAA. In any event, consent to such brazen data-collection activities must be specific and express. There is no disclosure or service agreement between Google and third-party

---

visited Nov. 11, 2020) (stating, "[t]hese terms reflect the parties' agreement with respect to the terms governing processing and security of Customer Data under the [Firebase Terms of Service for Firebase Services"] Agreement."). *See also* Terms of Service for Firebase Services, FIREBASE, https://firebase.google.com/terms (last visited Nov. 11, 2020) (stating, "I agree that my use of Firebase service is subject to the applicable terms below," including the "Firebase Data Processing and Security Terms").

[46] See also Google Ads Data Processing Terms, GOOGLE BUSINESSES AND DATA, https://privacy.google.com/businesses/processorterms/, Section 9, providing similar promises of honoring data subject rights and providing controls via "Data Subject Tool(s)" to control data collection (last visited Nov. 11, 2020).

[47] Firebase Data Processing and Security Terms, FIREBASE, https://firebase.google.com/terms/data-processing-terms#9.-data-subject-rights;-data-export (last visited Nov. 11, 2020), Section 5.1.3.

[48] The term is defined, in Google's terms, as "data protection or privacy legislation in force outside the European Economic Area, Switzerland, and the UK." Firebase Data Processing and Security Terms, FIREBASE, https://firebase.google.com/terms/data-processing-terms#9.-data-subject-rights;-data-export (last visited Nov. 11, 2020).

app developers that grants Google permission to intercept communications between users and apps when the user has turned off the WAA and/or sWAA features. And Google provided no notice to third-party app developers that it would intercept communications between users and apps when users shut off "Web & App Activity."

142. Further, nowhere in any disclosures did Google ever indicate to its users that any separate agreement, between Google and an app developer, might override the user's decision to turn off WAA and/or sWAA.

VI. Google Profits from the Communications It Intercepts [redacted], as Well as Data It Saves Relating to Users' Interactions with [redacted]

143. Google's continuous tracking of users is no accident. Google is one of the largest technology companies in the world. Google LLC and its parent Alphabet Inc. have over 1.5 billion active account users, and Alphabet Inc. boasts a net worth exceeding $1 trillion.

144. Google's enormous financial success results from its unparalleled tracking and collection of personal and sensitive user information (including Plaintiffs' and Class members'), which data Google then uses to target its advertisements.

145. Over the last five years, virtually all of Google's revenue was attributable to third-party advertising. Google is continuously driven to find new and creative ways to leverage users' data in order to sustain Google's phenomenal growth in its sales of advertising services.

146. Google profits from the data it collects and saves—including from users' interactions with [redacted] and third-party apps while users have switched off WAA and/or sWAA—in at least three ways. First, Google associates the confidential communications and data with a user profile or profiles. Second, Google later uses the user's profile (including the intercepted confidential communications at issue here) to direct targeted advertisements to consumers (including Plaintiffs and Class members) and track the impact of those advertisements on consumer behavior. [redacted] Google relatedly profits by leveraging data collected from non-Google apps by way of [redacted]

[redacted] Third, Google uses the results to modify Google's own algorithms and technology, such as Google Search.

A. Google Creates and Maintains "Profiles" on Its Users Using the Data Collected from Google [redacted]

147. Google builds and maintains "profiles" relating to each individual (including Plaintiffs and Class members) and to each of their devices. These "profiles" contain all the data Google can collect associated with each individual and each device. In a *Wired* article regarding Google's privacy practices, Professor Schmidt stated that Google's "business model is to collect as much data about you as possible and cross-correlate it so they can try to link your online persona with your offline persona. This tracking is just absolutely essential to their business. 'Surveillance capitalism' is a perfect phrase for it."[49]

148. Google uses those user profiles for numerous purposes. One important purpose is to guide Google's targeted advertisements. The profiles allow Google to effectively target advertisements. As a result of using the user profiles, Google's targeted advertisements are more effective and therefore Google can charge advertisers more for these services.

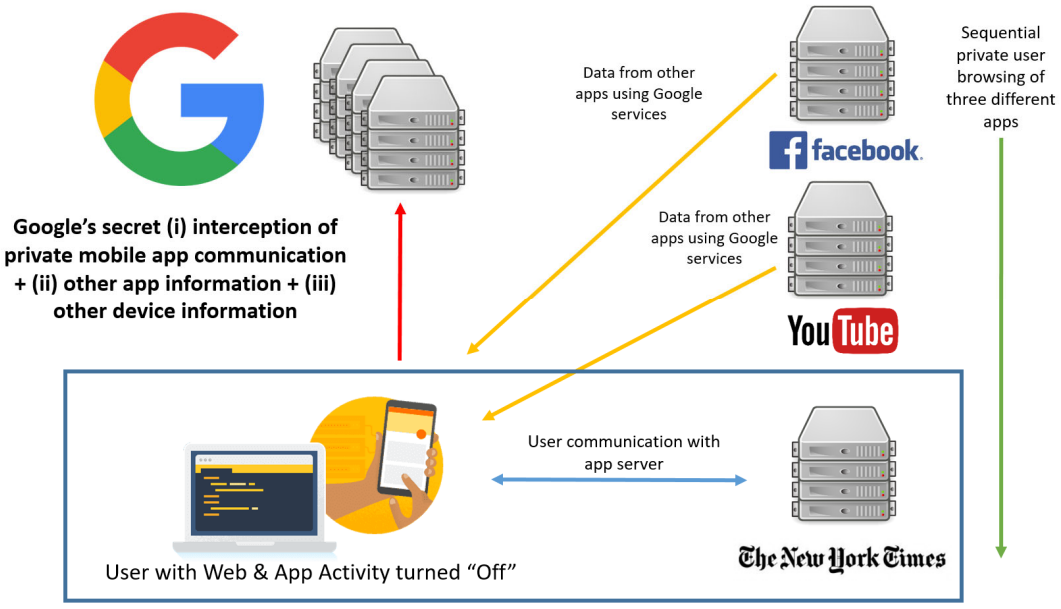
149. Google includes in its user profiles data secretly transmitted to Google from consumer devices by [redacted] during times that the user had switched off WAA and/or sWAA. Google also includes data that it saves from users' interactions with [redacted] while WAA was off. By including this data in its user profiles, Google increases the user profiles' value to Google and thereby allows Google to more effectively target advertisements to these users (among other uses of these profiles).

150. Google combines the data, including data transmitted to Google by Google [redacted], with additional data generated by apps, running on the device, including apps that use Google's services. This additional data includes: (1) device identifiers from the device's operating system; (2) geolocation information, including from cellular and wi-fi signals,

[49] Lily Hay Newman, *The Privacy Battle to Save Google from Itself*, WIRED (Nov. 1, 2018), https://www.wired.com/story/google-privacy-data/ (last visited Nov. 11, 2020).

and (3) Google's own persistent identifiers, such as its Google Analytics User-ID and Chrome X-Client Referrer Header, which identify specific individual users and the users' devices.

151. The following diagram illustrates the process by which Google collects information from a mobile device while users have WAA and/or sWAA turned off:



152. The communications and data transmitted to Google from consumer devices, including by [redacted], is not "anonymized" in any meaningful sense of that word. Instead, this data is combined by Google into a user profile with all the other detailed, user-specific data Google collects on individuals and their devices. Google then uses these detailed profiles to help generate billions of dollars in advertising revenues without users' consent.

B. Google Generates Targeted Advertising to Class Members Based on Data Transmitted to Google by [redacted]

153. Google's targeted advertising services generate the vast majority of Google's hundreds of billions of dollars in annual revenue.[50] The more accurately that Google can track and

[50] Eric Rosenberg, *How Google Makes Money (GOOG)*, INVESTOPEDIA (June 23, 2020), *available at* https://www.investopedia.com/articles/investing/020515/business-google.asp#:~:text=Google%20Ads%20and%20Search%20Advertising,results%20generated%20by%20Google's%20algorithm (last visited Nov. 11, 2020).

target consumers, the more advertisers are willing to pay.

154. Google's "Ad Manager" service generates targeted advertisements to be displayed alongside third-party websites' content. The "user profiles" described above are used by Ad Manager to select which ads to display to users.

155. Google also sells in-app advertising services. For example, some apps display an advertisement on part of the screen. Google is paid to select and transmit targeted advertisements in this way, as well. In doing so, Google uses the "user profiles" described above.

156. Google is able to demand high prices for its targeted-advertising services because Google's user profiles (including data that Google obtained from [redacted] are so detailed.

157. If Google were to give consumers (including Plaintiffs and Class members) power to shut off the stream of data transmission (including from [redacted]), then that would harm Google's ability to build detailed user profiles and to effectively target advertisements. That, in turn, would harm Google's biggest (by far) source of revenue. This explains why Google repeatedly promises privacy and control (in order to make users feel better) and then repeatedly breaks those promises (in order to make billions of dollars).

C. Google Refines and Develops Products Using the Data Transmitted to Google by the [redacted]

158. Google also benefits by using the data it collects and saves to refine existing Google products, services, and algorithms—and to develop new products, services, and algorithms. This collection, usage, and monetization of user data contravenes the steps Plaintiffs and Class members have taken to try to control their information and to prevent it from being used by Google.

1. Google Search

159. Currently, more than 90% of online searches carried out by U.S. consumers are done using Google's web-based search engine, called Google Search.

160. Google Search, and the algorithms that power it, make use of the data Google has obtained from the Google [redacted] transmissions at issue here. Google Search would not be nearly as effective without the activity data at issue here.

2. On-Device Search Features

161. Google also uses the [redacted] transmissions to develop and refine Google's "On-Device Search" services. "On-Device Search" refers to a search of the content contained, linked, or referred to in the various apps of a mobile device. On most devices, this function appears as a text rectangle, with a magnifying glass on the left side, and the word "Search" appearing where the user is meant to type in the query.

162. A well-built On-Device Search feature will not only allow users to find their tools and apps, but will also "deep link" the user to specific content and pages within the device's apps. These "deep links" are similar to how web-based searches, like Google Search, can take a user directly to specific pages within a website. If a user then selects a search result that is "deep linked" to content on an app, the phone will respond to that selection by opening the relevant app and taking the user to the relevant content within the app. This is in contrast to the more traditional Google Search function, which would only search *web pages* rather than searching *within apps.*

163. In 2015, an industry publication named *Search Engine Watch* described Google's On-Device Search as follows: "Google can index the content contained within an app, either through a sitemap file or through Google's Webmaster Tools. If someone searches for content contained within an app, and if the user has that app installed, the person then has the option to view that content within the app, as opposed to outside the app on a mobile webpage. For sites that have the same content on their main website and app, the app results will appear as deep links within the search listing. If the user has the app installed and they tap on these deep links, the app will launch and take them directly to the content."[51]

164. In order to make its On-Device Search function more powerful, Google collects and records the content of apps on users' phones. This is called "indexing." By "indexing" the contents of apps, Google makes On-Device search quicker and more accurate. In August 2015, Google-sponsored publication *Search Engine Land* announced:

$

[51] Christopher Ratcliff, *What Is App Indexing and Why Is It Important?*, SEARCH ENGINE WATCH (Nov. 19, 2015), *available at* https://www.searchenginewatch.com/2015/11/19/what-is-app-indexing-and-why-is-it-important/ (last visited Nov. 11, 2020).

> Historically, *app landing pages* on websites have been in the Google index—but *actual apps* and *internal app screens* have not…. Now that Google is indexing both app landing pages and deep screens in apps, Google's app rankings fall into two basic categories, App Packs and App Deep Links. App Packs are much more like the app search results that SEOs [search engine optimizers] are used to, because they link to app download pages in Google Play or the App Store, depending on the device that you are searching from."[52]

165. In March 2015, the industry publication *Readwrite* reported on a rival search function, called AppWords, that was outperforming Google in the market for On-Device Search:

> Deep links for mobile apps were designed to mimic Web links by letting users click into different parts of an app and not just its home screen. But they're also changing the way we discover new things. The deep-linking startup Deeplink has launched what appears to be the first intent based and keyword driven mobile search. Called AppWords (a play on Google AdWords), the new service basically prompts new links for app users to click on—ones that will take them from one app directly into another that's already on their phone. "Query-based search has become a secondary surfacing tool in mobile," said cofounder Noah Klausman. "AppWords uses context to predict what people want to search. What we've built is what Google should have built a long time ago."[53]

166. Google responded to this competition by acquiring Firebase in 2014, and then launching the Firebase SDK platform. Google intentionally designed the Firebase SDK scripts to copy and transmit, to Google, users' communications with the apps and app developers while overriding device and account level controls. Google did this because Google knew that it needed this data to develop and refine Google's On-Device Search services. The Firebase SDK scripts, and [redacted], give Google massive amounts of user data from apps—including apps that were developed for the devices of Google's rival, Apple.

167. When app developers use Firebase SDK and other Google services that rely on embedded [redacted], Google receives a number of benefits that enhance and

---

[52] Emily Grossman, *App Indexing & The New Frontier of SEO: Google Search + Deep Linking*, Search Engine Land (Aug. 12, 2015), *available at* https://searchengineland.com/app-indexing-new-frontier-seo-google-search-deep-linking-226517 (last visited Nov. 11, 2020).

[53] Lauren Orsini, *How Deep Linking Can Change the Way We Search on Mobile*, READWRITE.COM (Mar. 24, 2015), *available at* https://readwrite.com/2015/03/24/deep-linking-search-appwords/ (last visited Nov. 11, 2020).

reinforce its market power in the market for On-Device Search. As Google states in its own technical documentation for Firebase, Google's On-Device Search "uses information about the actions users take on public and personal content in an app to improve ranking for Search results and suggestions."

VII. The Communications Intercepted by Google Using Google [redacted]

168. The information Google has collected and saved from users (including by using Firebase SDK [redacted] is highly valuable to Google, to other technology and advertising companies, and to users. This value is well understood in the e-commerce industry.[54] The world's most valuable resource is no longer oil, but is instead consumers' data.[55]

169. Even before the Class Period, there was a growing consensus that consumers' personal data was very valuable. In 2004, Professor Paul M. Schwartz noted in the *Harvard Law Review*:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of

---

[54] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS No. 220 at 7 (Apr. 2, 2013), *available at* http://dx.doi.org/10.1787/5k486qtxldmq-en; *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD at 319 (Oct. 13, 2013), *available at* https://www.oecd.org/sti/inno/newsourcesofgrowthknowledge-basedcapital.htm; Pauline Glickman & Nicolas Glady, *What's the Value of Your Data?* TECHCRUNCH (Oct. 13, 2015), *available at* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Nov. 11, 2020) Paul Lewis & Paul Hilder, *Former Cambridge Analytica Exec Says She Wants Lies to Stop*, THE GUARDIAN (March 23, 2018), *available at* https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies (last visited Nov. 11, 2020); SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER at 166 (2019).

[55] *The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), *available at* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Nov. 11, 2020).

consumer information.[56]

170. Likewise, in 2011, Christopher Soghoian (a former fellow at the Open Society Institute and current principal technologist at the ACLU) wrote in *The Wall Street Journal*:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[57]

A. The Transmissions Are Valuable to Class Members

171. It is possible to quantify the cash value, to Class members, of the communications and data collected and saved by Google [redacted] while the WAA and/or sWAA features were turned off by Class members.

172. For example, in a study authored by Tim Morey, researchers studied the value that 180 internet users placed on keeping personal data secure.[58] Contact information was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. However, web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings:

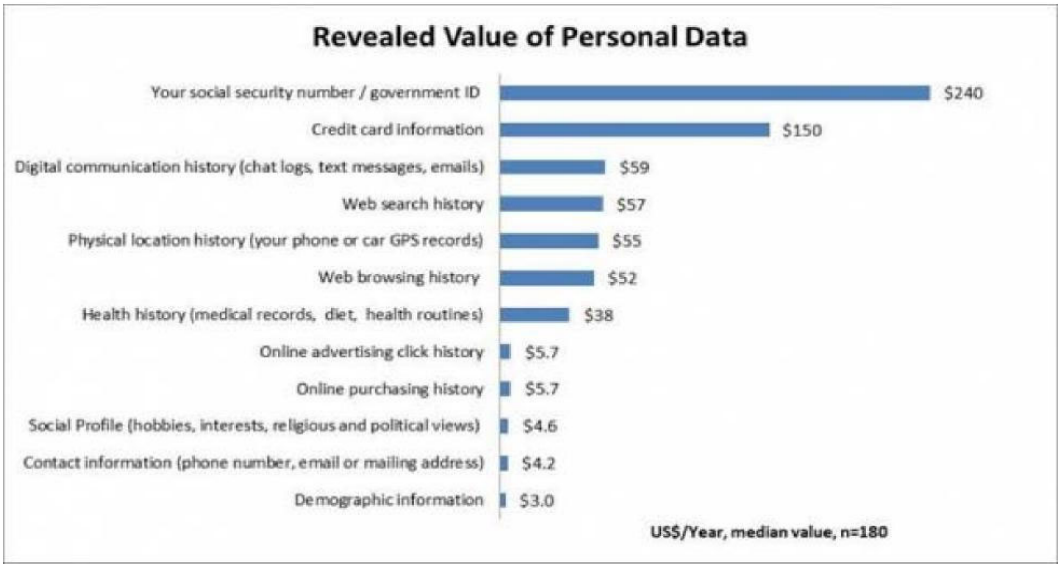
//

---

[56] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

[57] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011), *available at* https://www.wsj.com/articles/SB10001424052970204190704577024262567105738 (last visited Nov. 11, 2020).

[58] Tim Morey, *What's Your Personal Data Worth?*, DESIGN MIND (Jan. 18, 2011), *available at* https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html (last visited Nov. 11, 2020).



Although none of the categories on this chart corresponds directly to the data obtained by Google from Class members using the Firebase SDK scripts or other [redacted], Morey's research demonstrates that it is possible, in theory, to quantify the value of this data to users.

B. The Transmissions Are Valuable to Google

173. In addition to quantifying the value of the intercepted data *to users*, it is also possible to quantify the value of this data *to Google*.

174. For example, it is possible to calculate the profits Google has earned from using this data to enhance its "user profiles"; to sell targeted advertisements; and to develop and refine other Google products. *See supra*, ¶¶ 143-67.

175. It is also possible to assess the value of the intercepted data to Google by reference to the money that Google has, on other occasions, paid to users for this kind of data. Google began paying users for their web browsing data in 2012.[59]

176. Google also pays internet users to participate in a panel that Google calls "Google Screenwise Trends." The purpose of this panel is, according to Google, "to learn more about how

[59] Jack Marshall, *Google Pays Users for Browsing Data*, DIGIDAY (Feb. 10, 2012), *available at* https://digiday.com/media/google-pays-users-for-browsing-data/ (last visited Nov. 11, 2020); *see also* K.N.C., *Questioning the Searchers*, THE ECONOMIST (June 13, 2012), *available at* https://www.economist.com/schumpeter/2012/06/13/questioning-the-searchers (last visited Nov. 11, 2020).

everyday people use the Internet."

177. Upon becoming panelists for Google Screenwise Trends, these users add a browser extension that shares with Google the sites they visit and how they use them. The panelists consent to Google tracking such information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Barnes & Noble, Walmart, and Overstock.com. After three months, Google then pays panelists additional gift cards "for staying with" the panel.

178. These gift cards, mostly valued at $5, demonstrated that Google assigned cash value to the data it obtained from internet users' communications with the websites they visited. Google now pays Screenwise panelists up to $3 *per week*.

179. There are other ways to assess the value of this data, including in terms of Google's ability to maintain and extend its monopolies, as discussed below.

C. The Data Would Be Valuable to Other Internet Firms

180. The Firebase SDK and [redacted] transmissions at issue in this case would have value to other internet firms besides Google. The same is true for the data that Google saves from users' interactions with [redacted] It is possible to quantify this value.

181. During the Class Period, a number of platforms have appeared on which consumers monetize their data. For example:

a. Brave's web browser pays users to watch online targeted ads, while blocking out everything else.[60]

b. Loginhood "lets individuals earn rewards for their data and provides website owners with privacy tools for site visitors to control their data sharing," via a "consent

---

[60] Brandan Hesse, *Get Paid to Watch Ads in the Brave Web Browser*, LIFEHACKER (Apr. 26, 2019), *available at* https://lifehacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279#:~:text=Brave%2C%20a%20chromium-based%20web%20browser%20that%20boasts%20an,a%20more%20thoughtful%20way%20than%20we%E2%80%99re%20accustomed%20to (last visited Nov. 11, 2020) ("The model is entirely opt-in, meaning that ads will be disabled by default. The ads you view will be converted into Brave's cryptocurrency, Basic Attention Tokens (BAT), paid out to your Brave wallet monthly").

manager" that blocks ads and tracking on browsers as a plugin.[61]

c. Ex-presidential candidate Andrew Yang's "Data Dividend Project" aims to help consumers, "[t]ake control of your personal data. If companies are profiting from it, you should get paid for it."[62]

d. Killi is a new data exchange platform that allows users to own and earn from their data.[63]

e. BIGtoken "is a platform to own and earn from your data. You can use the BIGtoken application to manage your digital data and identity and earn rewards when your data is purchased."[64]

f. The Nielsen Company, famous for tracking the behavior of television viewers' habits, has extended its reach to computers and mobile devices through Nielsen Computer and Mobile Panel. These applications track consumers' activities on computers, phones, tablets, e-readers, and other mobile devices. In exchange, Nielsen gives users points worth up to $50 per month, plus the chance of winning more money in regular sweepstakes.[65]

---

[61] *Privacy Drives Performance*, LOGINHOOD, https://loginhood.io/ (last visited Nov. 11, 2020); *see also Chrome Browser Extension*, LOGINHOOD, https://loginhood.io/product/chrome-extension (last visited Nov. 11, 2020) ("Start earning rewards for sharing data – and block others that have been spying on you. Win-win.").

[62] *Your Data - Your Property*, DATA DIVIDEND PROJECT, https://www.datadividendproject.com/ (last visited Nov. 11, 2020) ("Get Your Data Dividend . . . . We'll send you $$$ as we negotiate with companies to compensate you for using your personal data.").

[63] *Killi Paycheck*, KILLI, https://killi.io/earn/ (last visited Nov. 11, 2020).

[64] *FAQ*, BIG TOKEN, https://bigtoken.com/faq#general_0 (last visited Nov. 11, 2020) ("Third-party applications and sites access BIGtoken to learn more about their consumers and earn revenue from data sales made through their platforms. Our BIG promise: all data acquisition is secure and transparent, with consumers made fully aware of how their data is used and who has access to it.").

[65] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, BEST WALLET HACKS (June 10, 2020), *available at* https://wallethacks.com/apps-for-selling-your-data/ (last visited Nov. 11, 2020).

g. Facebook has an app, called "Study," that pays users for their data. Facebook has another app, called "Pronunciations," that pays users for their voice recordings.[66]

182. As established by the California Constitution and the CCPA, and recognized by the recently-enacted California Privacy Rights and Enforcement Act, consumers have a property interest in their personal data. Not only does the CCPA prohibit covered businesses from discriminating against consumers that opt-out of data collection, the CCPA also expressly provides that: "[a] business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information." Cal. Civ. Code § 1798.125(b)(1). The CCPA provides that, "[a] business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature." Cal. Civ. Code § 1798.125(b)(4).

183. Through its false promises and unlawful data collection, Google is unjustly enriching itself.

184. If not for Google's actions, consumers could have received monetary value for their data from other internet firms.

D. There Is Value to Class Members in Keeping Their Data Private

185. In addition to monetary value of *selling* their data, Class members also assign value to keeping their data *private.* It is possible to quantify this privacy value, which is destroyed when the Firebase SDK scripts [redacted] surreptitiously transmit users' data to Google while the users have turned off WAA and/or sWAA. The privacy value is likewise destroyed when Google saves data relating to users' interactions with [redacted]

186. According to Google, more than 200 million people visit Google's "Privacy Checkup" website each year. Each day, nearly 20 million people check their Google privacy settings. Users do these things because they care about keeping their data private and preventing its disclosure to anyone else, including to Google.

---

[66] Jay Peters, *Facebook Will Now Pay You for Your Voice Recordings*, THE VERGE (Feb. 20, 2020), *available at* https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounnciations-app (last visited Nov. 11, 2020).

187. Users also switched off WAA and/or sWAA for the same reason—they cared about their privacy and wished to prevent anyone, including Google, from accessing their data.

188. Surveys of consumers indicate the importance that consumers assign to privacy. For example, in a recent study by the Pew Research Center, 93% of Americans said it was "important" for them to be "in control of who can get information" about them. Seventy-four percent said it was "very important." Eighty-seven percent of Americans said it was "important" for them not to have someone watch or listen to them without their permission. Sixty-seven percent said it was "very important." And 90% of Americans said it was "important" that they be able to "control[] what information is collected about [them]." Sixty-five percent said it was "very important" to control this.

189. Likewise, in a 2011 Harris Poll study, 76% of Americans agreed that "online companies, such as Google or Facebook, control too much of our personal information and know too much about our browsing habits."

VIII. Google Acted Without Consent to Intercept and Collect User Data to Maintain and Extend Its Monopolies

190. Google's audacious invasion of millions of users' privacy without consent was motivated in part by Google's ongoing efforts to unlawfully maintain and extend its monopoly power in search and other markets. These efforts included Google's 2014 acquisition of Firebase and Google's ongoing and unlawful interception, collection, and use of data when users have taken the affirmative step of turning off WAA and/or sWAA to prevent such interception, collection and use.

A. Google's Web Dominance

191. Since its founding in 1998, Google has developed technology allowing Google to constantly track consumers across the internet, fueling and then ensuring Google's search dominance. Over 90% of the U.S. population uses Google to conduct web searches, giving Google an enormous and unprecedented set of consumer data.

192. Google's dominance is tied to and based in part on Google's massive advertising business. Over 70% of online websites and publishers on the internet utilize Google's website

visitor-tracking product, "Google Analytics," which allows Google to track consumers.

193. To implement Google Analytics, Google requires websites to embed Google's custom code into their existing webpage code. Google's embedded code causes the user's browser to send his or her personal information to Google and its servers in California, such as the user's IP address, the URL address (which identifies the particular page of the website that is being visited), and other information regarding the user's device and browser.

194. By embedding its tracking code through Google Analytics, Google has been able to intercept, track, collect, take, compile, and use a staggering amount of consumer data, far more than any company in the world. Because more than 70% of websites use Google Analytics, Google is able to track and collect personal consumer data online in real time and on non-Google properties—more pervasively than any other company online.

195. Google has been able to maintain and extend its dominance in products like Google Search because no other company is able to track consumers and aggregate their communications with websites and throughout the internet like Google.

B. Google's Mobile Problem

196. Prior to 2007, with Apple's introduction of the iPhone, internet searching was primarily done on a computer, through a browser. With the 2007 launch of the iPhone, online activities began to move from computers to smartphones and the apps that run on them. This created an existential threat to Google's dominance.

197. Before Google acquired Firebase in October 2014, Google recognized that mobile applications on mobile devices allowed users to access information without using Google Search. Google thus knew that it needed data from users' app browsing activities to protect its search dominance and advertising revenues.

198. In February 2014, Google stated in its 10-K filings that one competitive threat to Google was "[m]obile applications on iPhone and Android devices, which allows users to access information directly from a publisher *without using our search engines*."

199. Google identified one of the key risk factors for the company as more people "using

devices other than desktop computers to access the internet" and acknowledged that "search queries are increasingly being undertaken via 'apps' tailored to particular devices or social media platforms, *which could affect our share of the search market over time*."

200. Google stated in its next series of 10-K filings that this risk was a threat to Google's lucrative advertising business, noting that "search queries are increasingly being undertaken via 'apps' tailored to particular devices or social media platforms, *which could affect our search and advertising business over time*."

C. Google's Mobile Focus with Android & Firebase

201. Google feared that consumers' switch from using computers to search, to instead using mobile devices to search, would endanger Google's dominance of the market for search functions. In response to that danger, Google adopted a new strategy: transport and embed Google's search ecosystem into every part of mobile devices over which Google had, or could gain, influence. Google's purpose in doing this was to keep fueling Google's dominance and advertising revenues.

202. One way Google sought to maintain and extend its dominance was with its acquisition of the Android operating system (OS); its subsequent development of Android; and its push to cause mobile device manufacturers to adopt Android on their devices. Google acquired Android in 2005 and released the first commercial version of the Android operating system, Android 1.0, in September 2008.

203. As recently recounted in the comprehensive report issued by the U.S. House of Representative's Subcommittee on Antitrust, Commercial and Administrative Law, entitled *Investigation of Competition In Digital Markets*, "[f]or mobile devices, Google imposed a set of restrictive contractual terms effectively requiring manufacturers of devices that used its Android operating system to pre-install both Chrome and Google Search."[67]

---

[67] STAFF OF S. COMM. ON ANTITRUST, COMMERCIAL, AND ADMINISTRATIVE LAW, INVESTIGATION OF COMPETITION IN DIGITAL MARKETS, at 178, https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519.

204. Just as Microsoft used its monopoly power on manufacturers to require the installation of Windows Explorer instead of Netscape, Google used its monopoly power to require phone manufacturers and app developers to incorporate Google's various products that reinforce Google Search. The more dominance Google could obtain in search, the more information it could collect and aggregate. The more information it could collect and aggregate, the more dominance Google could have in advertising, its key profit center.

205. One other way that Google sought to maintain and extend its dominance was with its October 2014 acquisition of Firebase; its subsequent development of the Firebase SDK platform; and its push to cause third-party app developers to adopt Firebase SDK. Before Google acquired it, Firebase was a separate company with an application programing interface (API) enabling synchronization of application data across Apple's iOS, Android, and web devices. By acquiring Firebase, Google gained the tools it needed to acquire users' mobile app data and, in part and along with Android, to address the competitive threat posed by Apple.

206. Firebase was so important to Google that the company featured it during Google's annual conference in May 2016, with Google CEO Sundar Pichai stating: "Firebase is the most comprehensive developer offering we have done to date." Google presented more than thirty sessions on Firebase during that 2016 conference.

207. During that conference, on May 20, 2016, Jason Titus, Vice President of Google's Developer Products Group, announced the "next generation of Firebase" with a mobile analytics tool called "Firebase Analytics" that was "inspired by much of the work that we've done in the last 10 years with Google Analytics, but it's designed specifically for the unique needs of apps."[68]

208. Google's Android and Firebase efforts are also tied to Google's efforts with "on device search." Because mobile apps are not constantly active on the device and need to be launched separately, it is much more difficult for Google to crawl and index content maintained on mobile content. Because of personal content and information, apps also tend to be secured,

[68] Pangambam S., *Google I/O 2016 Keynote (Full Transcript)*, THE SINGJU POST (May 20, 2016), *available at* https://singjupost.com/google-io-2016-keynote-full-transcript/?singlepage=1 (last visited Nov. 11, 2020).

self-contained, and separated from other apps. Unlike with data collection on the web, Google cannot simply send its army of "web crawlers" to scan, scrape, and store content with mobile apps.

209. Google's Firebase acquisition provided Google with what it previously lacked: the ability to collect personal user data *en masse* from mobile devices and apps—including devices and apps developed by its rival Apple. When app developers use Firebase SDK, Google receives a number of benefits that enhance and reinforce Google's market power. Firebase SDK enables Google to crawl and index apps just as it does for traditional websites. Developers often have no choice but to use Firebase SDK because of Google's demands and market power, including with search, analytics, advertisements, and the Android mobile operating system.

D. Google's Increasing Trove of Consumers' Mobile Data and Power

210. Since acquiring Firebase in 2014, Google has quietly collected what must be the largest index of mobile app pages in the world, including most apps on Android OS. Google has also continued to use its monopoly power with respect to web-based searching to push rapid adoption of Firebase SDK, so that it can eventually release a more complete search product that includes every mobile app page in the world. As a result, nearly every Android OS user (and most iOS users) are likely to have fallen victim to Google's unlawful acts.

211. Perhaps most concerning is that Google uses the data collected with Firebase SDK and other embedded [redacted]—including while users have WAA and/or sWAA turned off—to target users with advertisements throughout Google's entire advertising ecosystem—including in the very app where the communication was intercepted, and other apps of other app developers. All consumers' requests for content from the app thereby become accessible, collectible, and usable by Google, even where users have not consented to Google's collection and use of such information.

212. By compiling not just consumer profiles, but surveying human behavior across the vast majority of mobile app activity, Google tracks consumer activity more pervasively than any other company and is thus able to create a more targeted search product as compared to its competitors, by its ability to claim that Google knows how best to rank websites and online

properties. Google Search would not be nearly as potent a tool without Google Analytics as a complement and Google's ongoing data collection with its Firebase SDK [redacted] as well as Google's practice of saving information relating to users' interactions with [redacted]

213. Google's own internal documents reveal that Google knows what it is doing is wrong. But Google has made a bet: It has wagered that by the time regulators, lawmakers, or the public at large uncover that Google has compiled an almost unlimited amount of user data from apps (without proper consent), Google will have already won the game against any prospective competitor. Left unchecked, Google will achieve near complete monopoly power in search, data collection, and private user information the likes of which the world has never seen.

IX. Tolling of the Statutes of Limitations

214. Each unauthorized transmission of data to Google by the Firebase SDK scripts or [redacted] is a separate "wrong" which triggers anew the relevant statutes of limitations. The same is true of each specific datapoint related to users' interactions with [redacted], which Google impermissibly saves and uses.

215. Moreover, any applicable statutes of limitations have been tolled under (1) the fraudulent concealment doctrine, based on Google's knowing and active concealment and denial of the facts alleged herein, and (2) the delayed discovery doctrine, as Plaintiffs did not and could not reasonably have discovered Google's conduct alleged herein until shortly before the original complaint was filed.

216. Throughout the Class Period, Google repeatedly and falsely represented that its users (including Plaintiffs and Class members) could prevent Google from intercepting their communications by turning off WAA and/or sWAA. Google never disclosed that it would continue to track users and collect their data once this feature was turned off. Google also repeatedly and falsely represented that its users (including Plaintiffs and Class members) could prevent Google from saving information about their interactions with [redacted] by turning off WAA. Google never disclosed that it would continue to track users and save this data once this feature was turned off.

217. Google also further misled users by indicating that data associated with them would be viewable through their account, but Google did not make the user data at issue in this lawsuit (collected while WAA and/or sWAA is turned off) viewable in user accounts. Google's failure to do so during the Class period is part of Google's active deception and concealment.

218. Google has also made the statements quoted above, which (1) misrepresent material facts about Google's interception, storage, and use of users' data on apps and/or (2) omit to state material facts necessary to make the statements not misleading. *See supra*, ¶¶ 117-35. Google thereby took affirmative steps to mislead Plaintiffs and others about the effect of switching the WAA and/or sWAA features off.

219. Plaintiffs relied upon Google's false and misleading representations and omissions and believed that Google was not intercepting their private communications while the WAA and/or sWAA feature was turned off. Plaintiffs likewise relied upon Google's false and misleading representations and omissions and believed that Google was not saving information related to their interactions with [redacted] while the WAA feature was turned off.

220. Plaintiffs did not discover and could not reasonably have discovered that Google was instead intercepting, saving, and using their data in the ways set forth in this Complaint until shortly before the lawsuit was filed in consultation with counsel, and in some cases until after this lawsuit was filed and through discovery in this case.

221. Plaintiffs exercised reasonable diligence to protect their data from interception. That is precisely why they turned off the "Web & App Activity" feature: to protect their data from interception by Google, and to prevent Google from saving their data. Plaintiffs did not and could not reasonably have discovered their claims until consulting with counsel shortly before the filing of the original complaint through the exercise of reasonable diligence.

222. Accordingly, Plaintiffs and Class members could not have reasonably discovered the truth about Google's practices until shortly before this litigation was commenced.

X. Google Collected the Data for the Purpose of Committing Further Tortious and Unlawful Acts

223. Google collected and saved the data at issue here (from users who turned off WAA

and/or sWAA) for the purpose of committing additional tortious and unlawful acts. Google's subsequent use of the data violated the California Consumer Privacy Act ("CCPA"); the CDAFA; and the FTC's 2011 Consent Order. Google also used the data to tortiously invade consumers' privacy and intrude on their seclusion.

224. ***Google collected and saved the data with the intent to violate the California Consumer Privacy Act.*** The data collected from users at issue in this lawsuit, while Web & App Activity is turned off, qualifies as "personal information" that is protected by the CCPA. Cal. Civ. Code § 1798.140(o). The CCPA provides:

> "A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not . . . use personal information collected for additional purposes without providing the consumer with notice consistent with this section."

Cal. Civ. Code § 1798.100(b) (emphasis added).

225. At the time Google collected and saved data from users when they turned off WAA and/or sWAA, Google intended to "use" that data "for additional purposes without providing the consumer with notice consistent with this section." Whenever Google uses the confidential communications wrongfully collected or aggregates it with other information to gain additional insight and intelligence, Google has violated the express prohibitions of the CCPA.

226. Moreover, Google carried out its intent: As described elsewhere in this Complaint, Google made use of the data it collected from users who turned off WAA and/or sWAA for "additional purposes." The users had never been "informed" of those "additional purposes." Google never gave its users "notice consistent with" the CCPA's requirements regarding these "additional purposes" for which Google used the data collected from users who have turned off WAA and/or sWAA.

227. ***Google collected the data with the intent to violate the FTC's 2011 Consent Order.*** The FTC ordered Google to obtain "express affirmative consent" from each user, "prior to any new or additional sharing" of a user's information that is "a change from stated sharing practices in effect at the time [Google] collected such information."

228. Google began the data collection and sharing at issue in this lawsuit after the 2011 Consent Order. At the time Google collected data from users who turned off WAA and/or sWAA, Google intended to share that data with third parties, in a manner that was very different from the "stated sharing practices" Google had disclosed to users. Google intended to do this without obtaining consent.

229. Moreover, Google carried out its intent: Google shared and/or sold the data, collected from users who turned off WAA and/or sWAA with third-parties including Google's advertising customers. That sharing and/or selling of data contradicted Google's repeated assurances to users, described herein. Google shared this data without obtaining consent.

230. ***Google collected the data with the intent to violate the CDAFA.*** The CDAFA provides that it is a public offense to "without permission . . . make[] use of any data from a computer . . . ." Cal. Penal Code § 502.

231. At the time that Google caused the Firebase SDK [redacted] to transmit users' data to Google's servers, Google intended to later "make use of" that data to enhance Google's profiles on the users; to sell advertising services; to select and send targeted advertising; and for other purposes. Google then did "make use of" the data in these ways. These subsequent acts by Google were separate and independent violations of the CDAFA.

[redacted]

233. ***Google collected the data with the intent to intrude upon users' seclusion and invade their constitutional privacy.*** The California Constitution and common law protect consumers from invasions of their privacy and intrusion upon seclusion – in addition to newer privacy laws such as the CCPA.

234. Users of apps turned off WAA and/or sWAA for the purpose of preventing others, including Google, from finding out what the users were viewing and reading on mobile apps. For

example, users' app activities, while WAA and/or sWAA have been turned off, may reveal: a user's dating activity; a user's sexual interests and/or orientation; a user's political or religious views; a user's travel plans; a user's private plans for the future (e.g., purchasing of an engagement ring). These are just a few of the many intentions, desires, plans, and activities that users intend to keep private when they turn off WAA and/or sWAA.

[redacted]

236. Users had a reasonable expectation that Google would do as it promised, and that Google would stop collecting data from the Firebase SDK scripts and [redacted] once users switched off WAA and/or sWAA. Users likewise had a reasonable expectation that Google would stop saving data related to users' interactions with [redacted] once users switched off WAA.

237. By causing targeted advertisements to be sent to users and to users' devices, based on data Google collected and saved while users turned off WAA and/or sWAA, Google has caused that data to be revealed to others and has invaded the privacy and intruded upon the seclusion of the users whose data was collected and saved while they expected to have privacy.

238. Google had the intent to send these targeted advertisements at the time that Google was collecting data from users who turned off "Web & App Activity."

FACTUAL ALLEGATIONS REGARDING THE NAMED PLAINTIFFS

239. Google does not disclose all of the apps that use Firebase SDK and other [redacted], and for which Google therefore collected or continues to collect users' data while they have WAA and/or sWAA turned off, or the time period during which Google collected or continues to collect such data for any given app. Plaintiffs are therefore at this time

unable to identify all apps that are relevant for purposes of this litigation. Google's Firebase website identifies the following apps as supported by Firebase SDK: The New York Times, NPR One, Halfbrick, Duolingo, Alibaba, Lyft, Venmo, The Economist, Trivago, Ctrip, Wattpad, and Gameloft.[69] Other sources indicate that over 1.5 million apps use Google's Firebase SDK. Discovery will reveal which of Plaintiffs' apps were or are supported by Firebase SDK and other [redacted], and for which Google intercepted and collection data without disclosure of consent while WAA or sWAA was turned off.

240. Plaintiff Anibal Rodriguez is an adult domiciled in Florida and has active Google accounts and had active accounts during the Class Period.

241. Mr. Rodriguez's WAA and sWAA settings have been turned off for at least part of the Class Period.

242. Mr. Rodriguez has used [redacted] while his WAA setting has been turned off.

243. At various times during the Class Period, Mr. Rodriguez accessed numerous app pages on the Internet containing content he was interested in on his Android device while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Alarm Clock for Me, Alibaba, AliExpress, Amazon Shopping, Android TV, Applebee's, Aptoide, Assistant, Barcode Scanner, Baseball Superstars 2020, Best Buy, Burger King, Call of Duty, Chili's, ClassDojo, Clawee, Craigslist, Current, Dairy Queen, Domino's, DoorDash, Dosh, Drive, DroidCam, Duolingo, eBay, ES File Explorer, Fair, Fire TV, Fulldive VR, GIPHY, Glassdoor, GoMLS miami, GoodRx, Google Pay, Google Play Games, Groupon, Grubhub, Hangouts, Home, Ibotta, Indeed Job Search, Instagram, Instant Save, Jimmy John's, Kindle, Layout, Letgo, LinkedIn, Little Caesars, Lyft, McDonald's, MX Player, myCigna, Netflix, Ninja's Creed, OfferUp, Pandora, ParkMobile, PayPal, Pi Music Player, Pollo Tropical, Postmates, Prime Video, Publix, Publix Instacart, RaceTrac, RAR, Realtor.com, Repost, Retro Bowl, Samsung Members, Samsung Members v1, Samsung Notes, Samsung Pay, Samsung voice input, Sezzle,

[69] *See Firebase Helps Mobile and Web App Teams Succeed*, FIREBASE, https://firebase.google.com/.

Shazam, Shop, Shopping, Skillshare, Slack, Sleep Cycle, Slingshot Stunt Driver, Smart Switch, Sonos S1, SOPlayer, SoundCloud, Square Point of Sale, Stack Colors, Stash, Steam, Stickman Parkour Platform, Stream, Target, The Grand Mafia, Tiles Hop, Time Zone Updater, Trip.com, Trivago, Truebill, Uber, Uber Eats, Udemy, USPS Mobile, VeSyncFit, Voice, Voice Recorder, Walmart, WhatsApp, Wish, Word, WordPress, Xfinity, Xfinity Mobile, Xfinity My Account, Yelp, Your Phone Companion, YouTube Music, YouTube VR, Zelle, Zillow, ZipRecruiter, Zoho Mail, Zoom, Gmail, Google Calendar, Google Assistant, Google Fit, Google Pay, Google Shopping, Google Meet, Google Home, Google Chrome, Google, Google Maps, and Google TV. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. His communications with the apps that used Firebase SDK and other [redacted] were intercepted and tracked by Google without his knowledge or consent.

244. Plaintiff Sal Cataldo is an adult domiciled in New York and has active Google accounts had active Google accounts during the Class Period.

245. Mr. Cataldo's WAA and sWAA settings have been turned off for at least part of the Class Period.

246. Mr. Cataldo has used [redacted] while his WAA setting has been turned off.

247. At various times during the Class Period, Mr. Catalo accessed numerous app pages on the Internet containing content he was interested in on his Android devices while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Accuweather, Acrobat Reader, Amazon Shopping, Among Us, Aqua Mail, Audible, CBS Sports Fantasy, Chrome, Clock, Discord, Docs, Drive, ESPN, FuboTV, Gmail, IMDB, Instagram, Jaybird, Kindle, Lawnchair, Maps, MyFitnessPal, Nest, Noom, NPR News, NPR One, The New York Times, Outlook, PayPal, Photos, Play Music, Play Store, Pocket, Pocket Casts, Pokerrr 2, Premier League, Relay for Reddit, Samsung Internet, Samsung Notes, Sheets, Slack, Smokeball, Spotify, Talon, Tesla, Textra, The Athletic, The Economist, TheScore, Uber, Venmo, WalletHub, Waze, WhatsApp, Whole Foods, WHOOP, Wikipedia, Yahoo Fantasy, YouTube, Zero Calorie Counter, Zoom, Google Assistant, Google Chrome, Google Drive, Google Wallet, Google Files,

Gmail, Google, Google One, Google TV, Google Lens, Google Maps, Google Meet, Google News, Google Photos, Google Play Store, and Google Calendar. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. His communications with the apps that used Firebase SDK and [redacted] were intercepted and tracked by Google without his knowledge or consent.

248. Plaintiff Julian Santiago is an adult domiciled in Florida and has an active Google account and had an active Google account during the Class Period.

249. Mr. Santiago's WAA and sWAA settings have been turned off for at least part of the Class Period.

250. Mr. Santiago has used [redacted] while his WAA setting has been turned off.

251. At various times during the Class Period, Mr. Santiago accessed numerous app pages on the Internet containing content he was interested in on his Apple device while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Acorns, Amazon Shopping, Amazon Prime Video, Bleacher Report, Calm, Duolingo, E*Trade, ESPN Fantasy, Fundrise, Google Docs, Google Maps, Google Sheets, LinkedIn, MapMyRide, Marcus, Nextdoor, NFL, Nike Run Club, NPR One, Oak, Spotify, Starbucks, Stocks, Target, The Economist, Titan, Twitter, Venmo, Weather - The Weather Channel, Xfinity Stream, YouTube, and Google Maps. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. His communications with the apps that used Firebase SDK and other [redacted]e were intercepted and tracked by Google without his knowledge or consent.

252. Plaintiff Susan Lynn Harvey is an adult domiciled in California and has active Google accounts and had active Google accounts during the Class Period.

253. Ms. Harvey's WAA and sWAA settings have been turned off for at least part of the Class Period.

254. Ms. Harvey has used [redacted] while her WAA setting has been turned off.

255. At various times during the Class Period, Ms. Harvey accessed numerous app pages

on the Internet containing content she was interested in on her Android devices while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Avast Cleanup, Avast Antivirus – Scan & Remove Virus, Cleaner, Bixby Vision, California Lottery, Candy Crush, EECU, Facebook Messenger, File Viewer for Android, Galaxy Themes, Gangstar 4, Gold Fish, Google One, Jackpot Party, Jetpack, MixerBox, PicCollage, Samsung Gallery, Samsung Print Service Plugin, The New York Times, Voice Recorder, Wattpad, Gmail, Google Drive, Google Photos, Google Chrome, Google, Google Home, Google Play Store, YouTube, Google Maps, Google One, Google TV, Google Pay, and Google Meet. She sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. Her communications with the apps that used Firebase SDK and other [redacted] were intercepted and tracked by Google without her knowledge or consent.

256. None of the Plaintiffs consented to the interception, storage, and use of their confidential communications made while WAA and/or sWAA was turned off.

CLASS ACTION ALLEGATIONS

257. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the following Classes:

- Class 1 – All individuals who during the Class Period (a) turned off "Web & App Activity," or supplemental "Web & App Activity," and (b) whose mobile app activity (including [redacted] was still transmitted to Google, from (c) a mobile device running the Android operating system (OS), because of Google [redacted] including Firebase SDK and [redacted], on a non-Google branded mobile app.

- Class 2 – All individuals who during the Class Period (a) turned off "Web & App Activity," or "supplemental Web & App Activity," and (b) whose mobile app activity (including [redacted] was still transmitted to Google, from (c) a mobile device running a *non*-Android operating system (OS), because of [redacted], including Firebase SDK and [redacted], on a non-Google branded mobile app.

- Class 3 – All individuals who during the Class Period (a) turned off "Web & App Activity," (b) whose activity data related to interactions with [redacted] was still saved by Google, and (c) whose activity data related to interactions with [redacted] was used by Google for any purpose [redacted].

The Class Period begins on the date Google first received data from the device of a user who had turned off (or paused) WAA and/or sWAA, including as a result of [redacted] like the Firebase SDK scripts. The Class Period continues through the present.

258. Excluded from the Classes are: (1) the Court (including any Judge or Magistrate presiding over this action and any members of their families); (2) Defendant, its subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them have a controlling interest and its officers, directors, employees, affiliates, legal representatives; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel, Class counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

259. **Ascertainability**: Membership of the Classes is defined based on objective criteria and individual members will be identifiable from Google's records, including from Google's massive data storage, consumer accounts, and enterprise services. Based on information readily accessible to it, Google can identify members of the Classes who own an Android device or have a non-Android device with an associated Google account, who were victims of Google's impermissible interception, receipt, tracking, saving, or use of communications as alleged herein.

260. **Numerosity**: Each of the Classes likely consists of millions of individuals. Accordingly, members of the Classes are so numerous that joinder of all members is impracticable. Class members may be identified from Defendant's records, including from Google's consumer accounts and enterprise services.

261. **Predominant Common Questions**: Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Common questions for the Classes include, but are not limited to, the

following:

a. Whether Google represented that Class members could control what communications of user information, app history and activity data were intercepted, received, collected, saved, or used by Google;

b. Whether Google gave the Class members a reasonable expectation of privacy that their communications of user information, app history and activity data were not being intercepted, received, collected, saved, or used by Google when the Class member had WAA and/or sWAA turned off;

c. Whether Google in fact intercepted, received, collected, saved, or used communications of user information, app history and activity data from Class members when the Class members had WAA and/or sWAA turned off;

d. Whether Google's practice of intercepting, receiving, collecting, saving, or using communications of user information, app history and activity data violated state and federal privacy laws;

e. Whether Google's practice of intercepting, receiving, collecting, saving, or using communications of user information, app history and activity data violated state and federal anti-wiretapping laws;

f. Whether Google's practice of intercepting, receiving, collecting, saving, or using communications of user information, app history and activity data violated any other state and federal tort laws;

g. Whether Plaintiffs and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

h. Whether Plaintiffs and Class members have sustained damages as a result of Google's conduct and if so, what is the appropriate measure of damages or restitution.

262. **Typicality**: Plaintiffs' claims are typical of the claims of other Class members, as all members of the Classes were uniformly affected by Google's wrongful conduct in violation of federal and state law as complained of herein.

263. **Adequacy of Representation**: Plaintiffs will fairly and adequately protect the interests of the members of the Classes and have retained counsel that is competent and experienced in class action litigation, including nationwide class actions and privacy violations. Plaintiffs and their counsel have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class members. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so.

264. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of a single adjudication, economies of scale and comprehensive supervision by a single, able court. Furthermore, as the damages individual Class members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for Class members to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

265. **California Law Applies to the Entirety of Both Classes**: California's substantive laws apply to every member of the Classes, regardless of where in the United States the Class member resides, or to which Class the Class member belongs. Defendant's own Terms of Service explicitly state, "California law will govern all disputes arising out of or relating to these terms, service specific additional terms, or any related services, regardless of conflict of laws rules. These disputes will be resolved exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts."

266. By choosing California law for the resolution of disputes covered by its Terms of Service, Google concedes that it is appropriate for this Court to apply California law to the instant dispute to all Class members. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class members under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiffs and all Class members, thereby creating state interests that ensure that the choice

of California state law is not arbitrary or unfair. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible. The application of California laws to the Classes is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Classes and California has the greatest interest in applying its laws here.

267. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNTS

COUNT ONE: VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE § 502 *ET SEQ.*

268. Plaintiffs hereby incorporate Paragraphs 1 through 267 as if fully stated herein.

269. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Smart phone devices with the capability of using mobile apps are "computers" within the meaning of the statute.

270. Google violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, saving, analyzing, and using Plaintiffs' and Class members' data.

[redacted]

272. Despite Google's false representations to the contrary, Google effectively charged Plaintiffs, Class members, and other consumers and Google was unjustly enriched, by acquiring

their sensitive and valuable personal information without permission and using it for Google's own financial benefit, including to advance its advertising business. Plaintiffs and Class members retain a stake in the profits Google earned from their personal browsing histories and other data because, under the circumstances, it is unjust for Google to retain those profits.

273. Google accessed, copied, took, analyzed, and used data from Plaintiffs' and Class members' computers in and from the State of California, where Google: (1) has its principal place of business; and (2) used servers that provided communication links between Plaintiffs' and Class members' computers and Google, which allowed Google to access and obtain Plaintiffs' and Class members' data. Accordingly, Google caused the access of Plaintiffs' and Class members' computers from California and is therefore deemed to have accessed Plaintiffs' and Class members' computers in California.

274. As a direct and proximate result of Google's unlawful conduct within the meaning of Cal. Penal Code § 502, Google has caused loss to Plaintiffs and Class members in an amount to be proven at trial.

275. Google has been unjustly enriched in an amount to be proven at trial. [redacted]

276. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

277. Plaintiffs and Class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Google's violations were willful and, upon information and belief, Google is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

278. Plaintiffs and the Class members are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

COUNT TWO: INVASION OF PRIVACY

279. Plaintiffs hereby incorporate Paragraphs 1 through 267 as if fully stated herein.

280. The right to privacy in California's Constitution creates a right of action against private entities such as Google.

281. Plaintiffs' and Class members' expectation of privacy is deeply enshrined in California's Constitution. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

282. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone…It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.[70]

283. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Google.

284. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

285. As described herein, Google has intruded upon the following legally protected

---

[70] BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (Nov. 7, 1972).

privacy interests:

a. The California Invasion of Privacy Act as alleged herein;

b. A Fourth Amendment right to privacy contained on personal computing devices, including app-browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

c. The California Constitution, which guarantees Californians the right to privacy; and

d. Google's Privacy Policy and policies referenced therein and other public promises it made not to track or intercept the Plaintiffs' and Class members' communications or access their computing devices while WAA and/or sWAA were turned off.

286. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances in that Plaintiffs and Class members could not reasonably expect Google would commit acts in violation of federal and state civil and criminal laws; and Google affirmatively promised users (including Plaintiffs and Class members) it would not track their communications or access their computing devices and mobile apps while they turned off WAA and/or sWAA. Google also affirmatively promised users (including Plaintiffs and Class members) that it would not save information related to their interactions with [redacted] while they had turned off WAA.

287. Google's actions constituted a serious invasion of privacy in that it:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including search and browsing histories;

b. Violated several federal criminal laws

c. Violated dozens of state criminal laws on wiretapping and invasion of privacy, including the California Invasion of Privacy Act;

d. Invaded the privacy rights of millions of Americans (including Plaintiffs and class members) without their consent;

e. Constituted the unauthorized taking of valuable information from millions of Americans through deceit; and

f. Further violated Plaintiffs' and Class members' reasonable expectation of privacy via Google's saving, review, analysis, and subsequent uses of Plaintiffs' and Class members' private and other browsing activity that Plaintiffs and Class members considered sensitive and confidential; and

[redacted]

288. Committing criminal acts against millions of Americans constitutes an egregious breach of social norms that is highly offensive.

289. The surreptitious and unauthorized tracking, collection, saving, and/or use of the internet communications of millions of Americans, particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

290. Google's intentional intrusion into Plaintiffs' and Class members' internet communications and their computing devices and mobile apps was highly offensive to a reasonable person in that Google violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

291. The taking, saving, and use of personally-identifiable information from millions of Americans through deceit is highly offensive behavior.

292. Secret monitoring of mobile apps is highly offensive behavior.

[redacted]

294. Following Google's unauthorized interception and storage of the sensitive and valuable personal information, the subsequent analysis and use of that private data (including in conjunction with other data collected without authorization, from [redacted] or third-party apps) to develop and refine profiles on Plaintiffs, Class members, and consumers violated their reasonable expectations of privacy.

295. Wiretapping and surreptitious recording of communications is highly offensive behavior.

296. Google lacked a legitimate business interest in tracking users on their mobile apps without their consent.

297. Plaintiffs and Class members have been damaged by Google's invasion of their privacy and are entitled to just compensation and injunctive relief.

298. Google has been unjustly enriched in an amount to be proved at trial. [redacted]

COUNT THREE: INTRUSION UPON SECLUSION

299. Plaintiffs hereby incorporate Paragraphs 1 through 267 as if fully stated herein.

300. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

301. In carrying out its scheme to track and intercept Plaintiffs' and Class members' communications while they were using mobile apps with WAA and/or sWAA turned off, in violation of its own privacy promises, Google intentionally intruded upon the Plaintiffs' and Class members' solitude or seclusion in that it effectively placed itself in the middle of conversations to which it was not an authorized party. Google also intentionally intruded upon Plaintiffs' and Class members' solicitude or seclusion in that it saved, used, and profited from information that it promised not to save, including information related to their interactions with [redacted] while they had turned off WAA.

302. Google's tracking and interception were not authorized by Plaintiffs and Class members, the mobile app servers with which they were communicating, or even Plaintiffs' and Class members' mobile apps.

303. Google's intentional intrusion into Plaintiffs' and Class members' internet communications and their computing devices and mobile apps was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

304. The taking of personally-identifiable information from millions of Americans through deceit is highly offensive behavior, particularly where, as here, Plaintiffs and Class members took active (and recommended) measures to ensure their privacy.

305. Secret monitoring of internet activity is highly offensive behavior. The surreptitious and unauthorized tracking, collection, saving, and/or use of the internet communications of millions of Americans, particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

[redacted]

307. Wiretapping and surreptitious recording of communications is highly offensive behavior.

308. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person has their WAA and/or sWAA setting turned off.

309. Plaintiffs and the Class members have been damaged by Google's invasion of their privacy and are entitled to reasonable compensation including but not limited to disgorgement

of profits related to the unlawful internet tracking.

310. Google has been unjustly enriched in an amount to be proved at trial. [redacted]

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Appoint Plaintiffs to represent the Classes;

C. Appoint undersigned counsel to represent the Classes;

D. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

E. Award nominal damages to Plaintiffs and the Class members against Defendant;

F. Award punitive damages to Plaintiffs and the Class members against Defendant;

G. Non-restitutionary disgorgement of all of Defendant's profits that were derived, in whole or in part, from Google's interception, collection, saving, and subsequent use of Plaintiffs' communications;

H. Order Defendant to disgorge revenues and profits wrongfully obtained;

I. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from intercepting, tracking, collecting, saving, or using communications after Class members turned off WAA or sWAA, or otherwise violating its policies with users;

J. Award Plaintiffs and the Class members their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

K. Grant Plaintiffs and the Class members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: October 28, 2022

SUSMAN GODFREY LLP

/s/ Amanda Bonn
Amanda Bonn

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
Erika Nyborg-Burch, CA Bar No. 342125
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
brichardson@bsfllp.com
enyborg-burch@bsfll.com

Alison Anderson, CA Bar No. 275334
aanderson@bsfllp.com
BOIES SCHILLER FLEXNER LLP
725 S. Figueroa Street, 31st Floor
Los Angeles, CA 90017
Tel.: (213) 995-5720

Jesse Panuccio (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
1401 New York Ave, NW
Washington, DC 20005
Tel.: (202) 237-2727
Fax: (202) 237-6131
jpanuccio@bsfllp.com

James Lee (admitted *pro hac vice*)
Rossana Baeza (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307
jlee@bsfllp.com

rbaeza@bsfllp.com

John A. Yanchunis (admitted *pro hac vice*)
Michael F. Ram CA Bar No. 104805
Ryan J. McGee (admitted *pro hac vice*)
Ra Amen (admitted *pro hac vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
mram@forthepeople.com
rmcgee@forthepeople.com
ramen@forthepeople.com

William S. Carmody (admitted *pro hac vice*)
Shawn Rabin (admitted *pro hac vice*)
Steven M. Shepard (admitted *pro hac vice*)
Alexander P. Frawley (admitted *pro hac vice*)
Ryan K. Sila (admitted *pro had vice*)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019-6023
Tel.: (212) 336-8330
Fax: (212) 336-8340
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@ susmangodfrey.com
rsila@susmangodfrey.com

Ian B. Crosby (admitted *pro hac vice*)
Jenna G. Farleigh, CA Bar No. 288811
SUSMAN GODFREY L.L.P.
1201 Third Avenue Suite 3800
Seattle, WA 98101-3000
Tel: (206) 516-3880
Fax: (206) 516-3883
icrosby@susmangodfrey.com
jfarleigh@susmangodfrey.com

Attorneys for Plaintiffs

EXHIBIT A

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective July 1, 2020

Archived versions

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can contact us.

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

Things you create or provide to us

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

Go to Google Account

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.

Go to Ad Settings

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the Privacy Checkup, which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our Product Privacy Guide.

Go to Privacy Checkup

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

Privacy controls

Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

Go to Activity Controls

Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

Go to Ad Settings

About you

Control what others see about you across Google services.

Go to About You

Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

Go to Shared Endorsements

Information you share

If you're a G Suite user, control whom you share information with through your account on Google+.

Go to Information You Share

Ways to review & update your information

My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

Go to My Activity

Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

Go to Dashboard

Your personal information

Manage your contact information, such as your name, email, and phone number.

Go to Personal Info

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your YouTube Search History and your YouTube Watch History.
- Ad Settings: Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.

- Device-level settings: Your device may have controls that determine what information we collect. For example, you can modify location settings on your Android device.

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing an app in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to make a reservation through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email

- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

RETAINING YOUR INFORMATION

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as the content you create or upload. You can also delete activity information saved in your account, or choose to have it deleted automatically after a set period of time.
- Other data is deleted or anonymized automatically after a set period of time, such as advertising data in server logs.
- We keep some data until you delete your Google Account, such as information about how often you use our services.
- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form. We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

You can read more about Google's data retention periods, including how long it takes us to delete your information.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

California requirements

The California Consumer Privacy Act (CCPA) requires specific disclosures for California residents.

This Privacy Policy is designed to help you understand how Google handles your information:

- We explain the categories of information Google collects and the sources of that information in Information Google collects.
- We explain how Google uses information in Why Google collects data.
- We explain when Google may share information in Sharing your information. Google does not sell your personal information.

The CCPA also provides the right to request information about how Google collects, uses, and discloses your personal information. And it gives you the right to access your information and request that Google delete that information. Finally, the CCPA provides the right to not be discriminated against for exercising your privacy rights.

We describe the choices you have to manage your privacy and data across Google's services in Your privacy controls. You can exercise your rights by using these controls, which allow you to access, review, update and delete your information, as well as export and download a copy of it. When you use them, we'll validate your request by verifying that you're signed in to your Google Account. If you have questions or requests related to your rights under the CCPA, you (or your authorized agent can also contact Google.

The CCPA requires a description of data practices using specific categories. This table uses these categories to organize the information in this Privacy Policy.

Categories of personal information we collect

Identifiers such as your name, phone number, and address, as well as unique identifiers tied to the browser, application, or device you're using.

Demographic information, such as your age, gender and language.

Commercial information such as your payment information and a history of purchases you make on Google's services.

Biometric information if you choose to provide it, such as fingerprints in Google's product development studies.

Internet, network, and other activity information such as your search terms; views and interactions with content and ads; Chrome browsing history you've synced with your Google Account; information about the interaction of your apps, browsers, and devices with our services (like IP address, crash reports, and system activity); and activity on third-party sites and apps that use our services. You can review and control activity data stored in your Google Account in My Activity.

Geolocation data, such as may be determined by GPS, IP address, and other data from sensors on or around your device, depending in part on your device and account settings. Learn more about Google's use of location information.

Audio, electronic, visual and similar information, such as voice and audio information when you use audio features.

Professional, employment, and education information, such as information you provide or that is maintained through a G Suite account by an organization at which you study or work.

Other information you create or provide, such as the content you create, upload, or receive (like photos and videos or emails, docs and spreadsheets. Google Dashboard allows you to manage information associated with specific products.

Inferences drawn from the above, like your ads interest categories.

Business purposes for which information may be used or disclosed

Protecting against security threats, abuse, and illegal activity: Google uses and may disclose information to detect, prevent and respond to security incidents, and for protecting against other malicious, deceptive, fraudulent, or illegal activity. For example, to protect our services, Google may receive or disclose information about IP addresses that malicious actors have compromised.

Auditing and measurement: Google uses information for analytics and measurement to understand how our services are used, as well as to fulfill obligations to our partners like publishers, advertisers, developers, or rights holders. We may disclose non-personally identifiable information publicly and with these partners, including for auditing purposes.

Maintaining our services: Google uses information to ensure our services are working as intended, such as tracking outages or troubleshooting bugs and other issues that you report to us.

Research and development: Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google's language models and build features like Google Translate.

Use of service providers: Google shares information with service providers to perform services on our behalf, in compliance with our Privacy Policy and other appropriate confidentiality and security measures. For example, we may rely on service providers to help provide customer support.

Advertising: Google processes information, including online identifiers and information about your

interactions with advertisements, to provide advertising. This keeps Google's services and many of the websites and services you use free of charge. You can control what information we use to show you ads by visiting your ad settings.

Legal reasons: Google also uses information to satisfy applicable laws or regulations, and discloses information in response to legal process or enforceable government requests, including to law enforcement. We provide information about the number and type of requests we receive from governments in our Transparency Report.

Parties with whom information may be shared

Other people with whom you choose to share your information, like docs or photos, and videos or comments on YouTube.

Third parties to whom you consent to sharing your information, such as services that integrate with Google's services. You can review and manage third party apps and sites with access to data in your Google Account.

Service providers, trusted businesses or persons that process information on Google's behalf, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

Domain administrators, if you work or study at an organization that uses Google services like G Suite.

Law enforcement or other third parties, for the legal reasons described in Sharing your information.

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- Chrome & the Chrome Operating System
- Play Books
- Payments
- Fiber
- Google Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link, for Children under 13 (or applicable age in your country)
- Voice and Audio Collection from Children's Features on the Google Assistant

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- Your Google Account is home to many of the settings you can use to manage your account
- Privacy Checkup guides you through key privacy settings for your Google Account
- Google's safety center helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- Privacy & Terms provides more context regarding this Privacy Policy and our Terms of Service
- Technologies includes more information about:
  - How Google uses cookies
  - Technologies used for Advertising
  - How Google uses pattern recognition to recognize things like faces in photos
  - How Google uses information from sites or apps that use our services

---

Key terms

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the companies providing business services in the EU.

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Google Account

You may access some of our services by signing up for a Google Account and providing us with some personal information (typically your name, email address, and a password. This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Referrer URL

A Referrer URL (Uniform Resource Locator is information transmitted to a destination webpage by a web browser, typically when you click a link to that page. The Referrer URL contains the URL of the last webpage the browser visited.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These “server logs” typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for “cars” looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 -
740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user’s ISP. Depending on the user’s service, a different address may be assigned to the user by their service provider each time they connect to the Internet.
- `25/Mar/2003 10:15:32` is the date and time of the query.
- `http://www.google.com/search?q=cars` is the requested URL, including the search query.
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used.
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they’ve visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. Learn more about how Google uses cookies.

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be managed in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID, such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.

Additional Context

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more about Google ads and why you may see particular ads.

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

combine the information we collect

Some examples of how we combine the information we collect include:

- When you're signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. Learn more

- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. Learn more

- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based your activity. Learn more

- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. Learn more

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can learn more here. You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can search and browse privately or turn off signed-out search personalization.

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video

- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account

- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. Learn more

- A flight confirmation email you receive may be used to create a “check-in” button that appears in your Gmail

- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

devices

For example, we can use information from your devices to help you decide which device you’d like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

Information about things near your device

If you use Google’s Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google’s Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-

Fi access points (like MAC address and signal strength. All these things help to determine your location. You can use your device settings to enable Google Location services. Learn more

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our Transparency Report.

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. Learn more

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. Learn more

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information,

like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. Learn more

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. Learn more

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. Learn more

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account.

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

rely on cookies to function properly

For example, we use a cookie called 'lbcs' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. Learn more

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The “last account activity” feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. Learn more

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel.” We don’t use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

servers around the world

For example, we operate data centers located around the world to help keep our products continuously available for users.

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail

- Google Fi, for a phone plan

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. Learn more

specific Google services

For example, you can delete your blog from Blogger or a Google Site you own from Google Sites. You can also delete reviews you've left on apps, games, and other content in the Play Store.

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. Learn more about these partners and how they use your information.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. Learn more

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you contact most frequently.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense or analytics tools (like Google Analytics, or it might embed other content (such as videos from YouTube. These services may share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services, this data may be associated with your personal information.

Learn more about how Google uses data when you use our partners' sites or apps.